AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT	1. CONTRACT ID CODE	PAGE 1 OF 2

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
PS36		21434781	

6. ISSUED BY	CODE 47QFCA	7. ADMINISTERED BY (If other than item 6)	CODE
GSA/FEDSIM Acquisition (QF0B1D) 1800 F Street, NW, 3100 Washington, DC 20405 Contract Specialist Name: Charlesetta D Ward Contract Specialist Phone: 999-999-9999			

8. NAME AND ADDRESS OF CONTRACTOR (No., Street, County, State and ZIP Code)	(X)	9A. AMENDMENT OF SOLICITATION NO.
LOCKHEED MARTIN CORPORATION 9500 GODWIN DR MANASSAS, VA, 20110-4166 Phone: (703) 367-3599 Fax: (703) 367-6319		9B. DATED (SEE ITEM 11)
	X	10A. MODIFICATION OF CONTRACT/ORDER NO. GS00Q09BGD0011 / GSQ0017AJ0021
		10B. DATED (SEE ITEM 13) 01/18/2017
CODE FACILITY CODE		

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing items 8 and 15, and returning ____ copies of the amendment; (b) By acknowledge receipt of this amendment on each of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment your desire to change an offer already submitted, such change may be made by telegram or letter provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and data specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

285F.Q00FB000.AA10.25.AF151.H08 Total Amount of MOD: ($50,000.00)

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
X	D. OTHER (Specify type of modification and authority) **FAR 52.243-2 Changes Cost-Reimbursement.**

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return ____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this modification is to 1)Realign Ceiling, 2) Deobligate FY20 Funding, 3) Update COR, 4) Update Version Date of FAR Clause, 5) Update IFT, 6) Update AFDP, and 7) Update Appendix A Service Levels. Please see SF30 Continuation Page for further detailed information.

Except as provided herein, all terms and conditions of the document referenced in item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
Mary L. Galbraith Contract Mgr		**Andrew R Hotaling**	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
(Signature of person authorized to sign)	9/21/2020	(Signature of Contracting Officer)	

		PAGES

Line Item Summary							
ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	Rev. Ext. Price (F)	Prev. Ext. Price (G)	Amount Of Change (H)
0001	**Base Year CPAF labor**	[redacted]					
0002	**Base Year CPAF Surge labor**						
0003	**Base Year Long Distance Travel**						
0004	**Base Year Tools**						
0005	**Base Year Other Direct Costs**						
0006	**Base Year Contract Access Fee**						
1001	**Option Period 1 Labor**						
1002	**Option Period 1 Surge Labor**						
1003	**Option Period 1 Long Distance Travel**						
1004	**Option Period 1 Tools**						
1005	**Option Period 1 ODCs**						
1006	**Option Period 1 Contract Access Fee (CAF)**						
2001	**Option Period 2 Labor**						
2002	**Option Period 2 Surge Labor**						
2003	**Option Period 2 Long Distance Travel**						
2004	**Option Period 2 Tools**						
2005	**Option Period 2 ODCs**						
2007	**Option Period 2 CAF**						
3001	**Option Period 3 Labor (Tasks 1-11)**						
3002	**Option Period 3 Surge Labor**						
3003	**Option Period 3 Travel**						
3004	**Option Period 3 Tools**						
3005	**Option Period 3 ODCs**						
3006	**Option Period 3 CAF**						
				TOTALS:	[redacted]		**($50,000.00)**

SF 30 Continuation Page
Task Order GSQ0017AJ0021
Modification PS36

Block 14 Continued

Purpose of Modification

1. Realign Unfunded Ceiling.
2. Deobligate FY20 Funding.
3. Update Contract Officer Representative (COR).
4. Update Version Date of Federal Acquisition Regulation (FAR) Clause.
5. Update Incremental Funding Table, Attachment H.
6. Update Award Fee Determination Plan, Attachment I.
7. Update Appendix A Service Levels, Attachment J.

Summary of Modification

1. Realign unfunded ceiling in the total amount of $13,700,000.00. SECTION B updated as follows (see Incremental Funding Table, Attachment C for estimated cost, estimated base fee, and estimated award fee):

DECREASED

- CLIN 0002 (BP Surge Labor) ceiling has **DECREASED** by (b) (4) **from** (b) (4) **to** (b) (4)
- CLIN 0004 (BP Tools) ceiling has **DECREASED** by (b) (4) **from** (b) (4) **to** (b) (4)
- CLIN 1002 (OP1 Surge Labor) ceiling has **DECREASED** by (b) (4) **from** (b) (4) **to** (b) (4)
- CLIN 2001 (OP2 Labor) ceiling has **DECREASED** by (b) (4) **from** (b) (4) **to** (b) (4)
- CLIN 2002 (OP2 Surge Labor) ceiling has **DECREASED** by (b) (4) **from** (b) (4) **to** (b) (4)
- CLIN 2004 (OP2 Tools) ceiling has **DECREASED** by (b) (4) **from** (b) (4) **to** (b) (4)
- CLIN 2005 (OP2 ODC) ceiling has **DECREASED** by (b) (4) **from** (b) (4) **to** (b) (4)

INCREASED

- CLIN 3001 (OP3 Labor) ceiling has **INCREASED** by (b) (4) **from** (b) (4) **to** (b) (4)

- CLIN 3002 (OP3 Surge Labor) ceiling has **INCREASED** by (b) (4) **from** (b) (4) **to** (b) (4)
- CLIN 3004 (OP3 Tools) ceiling has **INCREASED** by (b) (4) **from** (b) (4) **to** (b) (4)
- CLIN 3005 (OP3 ODC) ceiling has **INCREASED** by (b) (4) **from** (b) (4) **to** (b) (4)

Table 1: MOD 36 Realignments

CLIN	Current Ceiling	Change	New Ceiling
0002	(b) (4)		
0004			
1002			
2001			
2002			
2004			
2005			
3001			
3002			
3004			
3005			

2. Deobligate FY20 Funding from CLIN 3004 (OP3 Tools) as follows:

- CLIN 3004 (OP3 Tools) funding is **DECREASED** by (b) (4) **from** (b) (4) **to** (b) (4)

Table 2: MOD 36 MIPR

Source	MIPR	OMIS TO	IAA	$ to Obligate	Account	FY of Funds	CLINs
OSD DAMO	HQ0642923566	2016006B7	76	($50,000.00)	2016006DE-3048	FY20	3004

As a result of the above change in funding, Section B.5.3.1 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION is modified as follows:

"Incremental funding in the amount of $252,056,449.72 for CLINs 0001 through 3006 is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs may be allotted and available for payment by the Government as the funds become available. The estimated period of performance covered by the allotments for the mandatory CLINs is from award through January 18, 2021. The TO may be modified to add funds incrementally up to the maximum of $282,262,840 over the performance period of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by CLIN basis."

3. In Sections F.6 – F.7 PLACES OF DELIVERY and G.1.1. CONTRACT ADMINISTRATION of the Task Order, remove the current Contracting Officer's Representative (COR) and update the current Alternate Contracting Officer's Representative (ACOR) to the COR as follows:

Contracting Officer's Representative (COR):
Bonnie Heider
GSA FAS AAS FEDSIM (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: (202) 676-7136 (mobile)
Email: bonnie.heider@gsa.gov

4. In Section I.2 of the Conformed Task Order, update the version date of Federal Acquisition Regulation (FAR) clause 52.204-25 ("Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment") from "August 2019" to "August 2020."

5. Update the Incremental Funding Table as Attachment H.

6. Update Award Fee Determination Plan, Attachment I as follows:

On Attachment I - Award Fee Determination Plan, table 4.2 Second and Subsequent Award Fee Evaluation Period enter the on the line Option Year 3 Period 7 the following values:

a. Cost Incurred (if Planned Value not available): (b) (4)
b. Award Fee Pool Allocation: (b) (4)
c. Earned Award Fee: (b) (4)

d. Unearned Fee: (b) (4)

Table 3: MOD 36 Award Fee Determination Plan (Table 4.2)

Year	Period	Planned Value (Estimated Cost + Award Fee)	Cost Incurred (if Planned Value not available)	Award Fee Pool Allocation	Earned Award Fee	Unearned Fee
Base Year	1	(b) (4)				
Base Year	2					
Option Year 1	3					
Option Year 1	4					
Option Year 2	5					
Option Year 2	6					
Option Year 3	7					
Option Year 3	8					
Option Year 4	9					
Option Year 4	10					

On Attachment I Award Fee Determination Plan, Section 6.2 Award Fee Evaluation Board (AFEB) replace the COR's name with Bonnie Heider and the Contracting Officer's name with Andrew Hotaling. See Table 3 below.

Table 4: MOD 36 Award Fee Determination Plan (Section 6.2, AFEB)

Board Position	Title/Role	Name
AFEB Chairperson	DC3 BTO Representative	Matthew Rout
AFEB Voting Member	DC3 CFL Representative	Michael Ricucci
AFEB Voting Member	DC3 TSD Representative	Joan Donahue
AFEB Voting Member	DC3 DCISE Representative	Krystal Covey
AFEB Voting Member **	DC3 AG Representative	John Morcomb
AFEB Voting Member **	DC3 ITD Representative	Christopher Aiken
AFEB Voting Member **	DC3 DVP Representative	Kris Johnson
AFEB Voting Member	FEDSIM COR	Bonnie Heider
AFEB Non-Voting Member	FEDSIM Contracting Officer	Andrew Hotaling
AFEB Non-Voting Member	FEDSIM Contract Specialist	Charlie Ward

7. Update Attachment J Appendix A Service Levels spreadsheet.

SUMMARY OF CHANGES

All changes are annotated by a vertical line on the right margin of the Task Order.

All other terms and conditions remain unchanged and in effect.

The total obligated funding is **DECREASED** by (b) (4) **from** (b) (4) **to** (b) (4)

The Task Order ceiling remains unchanged at $347,479,403.00.

END OF MODIFICATION

TASK ORDER

GSQ0017AJ0021

MISSION SUPPORT

in support of:

DEFENSE CYBER CRIME CENTER (DC3)

Issued to:

Lockheed Martin Corporation
9500 Godwin Drive
Manassas, VA 20110

Under ALLIANT Contract# GS00Q09BGD0011

Issued by:
The Federal Systems Integration and Management Center (FEDSIM) 1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405

January 18, 2017

FEDSIM Project Number DE00789

B.1 GENERAL

The work shall be performed in accordance with all Sections of this Task Order (TO) and the contractor's Basic Contract, under which the resulting TO will be placed. An acronym listing to support this Task Order Request (TOR) is included in **Section J, Attachment K**.

B.2 CONTRACT ACCESS FEE (CAF)

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a CAF. In accordance with the Alliant base contract, the CAF shall be 0.75 percent of the total TO value with a cap of $100,000 per year per order (when order is in excess of $13.3 million (M) per order year). This TO shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO award.

B.3 ORDER TYPES

The contractor shall perform the effort required by this TO on a Cost-Plus-Award-Fee (CPAF) basis for Mandatory CLINs x001 and Optional CLINs x002 and Not-to-Exceed (NTE) basis for CLINs x003, x004, x005, and x006. The work shall be performed in accordance with all Sections of this TO and the offeror's Basic Contract, under which the resulting TO will be placed.

B.4 SERVICES AND PRICES/COSTS

Long-distance travel is defined as travel over 50 miles from your primary place of performance that includes all DC3 official work places (911 Elkridge Landing Rd Landing Rd, Linthicum Heights, Maryland 21090, National Media Exploitation Center (NMEC) in Northern Virginia, the NCIJTF in Chantilly, Virginia (VA) and the DIB in Alexandria, VA) . Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CLIN	Contract Line Item Number
CPAF	Cost-Plus-Award-Fee
NTE	Not-to-Exceed
ODC	Other Direct Cost

B.4.1 BASE PERIOD: MANDATORY LABOR CLIN

CLIN	Description	Cost	Base Fixed Fee	Award Fee	Total CPAF
0001	Labor (Tasks 1-11)	(b) (4)	[redacted]	[redacted]	$42,333,724

OPTIONAL SURGE CLIN

CLIN	Description	Cost	Base Fixed Fee	Award Fee	Total CPAF
0002	Labor (Task 12)	(b) (4)	[redacted]	[redacted]	$1,972,269

COST REIMBURSEMENT TRAVEL, TOOLS, and ODCs CLINs

CLIN	Description		Total NTE Price
0003	Long-Distance Travel Including G&A (b) (4)	NTE	$ 100,000.00
0004	Tools Including Indirect Handling Rate (b) (4)	NTE	$16,225,139
0005	ODCs Including Indirect Handling Rate (b) (4)	NTE	$ 500,000.00

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
0006	Contract Access Fee	NTE	$100,000

TOTAL CEILING BASE PERIOD CLINs: **$61,231,132**

B.4.2 FIRST OPTION PERIOD:

MANDATORY LABOR CLIN

CLIN	Description	Cost	Base Fixed Fee	Award Fee	Total CPAF
1001	Labor (Tasks 1-11)	(b) (4)	[redacted]	[redacted]	$50,169,672

OPTIONAL SURGE CLIN

CLIN	Description	Cost	Base Fixed Fee	Award Fee	Total CPAF
1002	Labor (Task 12)	(b) (4)	[redacted]	[redacted]	$3,823,314

COST REIMBURSEMENT TRAVEL, TOOLS, and ODCs CLINs

CLIN	Description		Total NTE Price
1003	Long-Distance Travel Including G&A (b) (4)	NTE	$ 100,000
1004	Tools Including Indirect Handling Rate (b) (4)	NTE	$ 12,760,823
1005	ODCs Including Indirect Handling Rate (b) (4)	NTE	$ 1,570,000

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
1006	Contract Access Fee	NTE	$100,000

TOTAL CEILING FIRST OPTION PERIOD CLINs: $ 68,523,809

B.4.3 SECOND OPTION PERIOD:

MANDATORY LABOR CLIN

CLIN	Description	Cost	Base Fixed Fee	Award Fee	Total CPAF
2001	Labor (Tasks 1-11)	(b) (4)	[redacted]	[redacted]	$52,600,826

OPTIONAL SURGE CLIN

CLIN	Description	Cost	Base Fixed Fee	Award Fee	Total Cost Plus Award
2002	Labor (Task 12)	(b) (4)	[redacted]	[redacted]	$4,131,238

COST REIMBURSEMENT TRAVEL, TOOLS and ODCs CLINs

CLIN	Description		Total NTE Price
2003	Long-Distance Travel Including G&A (b) (4)	NTE	$ 100,000
2004	Tools Including Indirect Handling Rate (b) (4)	NTE	$ 9,500,000
2005	ODCs Including Indirect Handling Rate (b) (4)	NTE	$ 1,000,000

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
2006	Contract Access Fee	NTE	$100,000

TOTAL CEILING SECOND OPTION PERIOD CLINs: $ 67,432,064

B.4.4 THIRD OPTION PERIOD: MANDATORY LABOR CLIN

CLIN	Description	Cost	Base Fixed Fee	Award Fee	Total CPAF
3001	Labor (Tasks 1-11)	(b) (4)	[redacted]	[redacted]	$58,790,428

OPTIONAL SURGE CLIN

CLIN	Description	Cost	Base Fixed Fee	Award Fee	Total CPAF
3002	Labor (Task 12)	(b) (4)	[redacted]	[redacted]	$7,285,407

COST REIMBURSEMENT TRAVEL, TOOLS and ODCs CLINs

CLIN	Description		Total NTE Price
3003	Long-Distance Travel Including G&A Rate (b) (4)	NTE	$ 100,000.00
3004	Tools Including Indirect Handling Rate (b) (4)	NTE	$ 16,800,000
3005	ODCs Including Indirect Handling Rate (b) (4)	NTE	$ 2,000,000

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
3006	Contract Access Fee	NTE	$100,000

TOTAL CEILING THIRD OPTION PERIOD CLINs: $ 85,075,835

B.4.5 FOURTH OPTION PERIOD: MANDATORY LABOR CLIN

CLIN	Description	Cost	Base Fixed Fee	Award Fee	Total Cost Plus
4001	Labor (Tasks 1-11)	(b) (4)	[redacted]	[redacted]	$50,486,517

OPTIONAL SURGE CLIN

CLIN	Description	Cost	Base Fixed Fee	Award Fee	Total CPAF
4002	Labor (Task 12)	(b) (4)	[redacted]	[redacted]	$1,430,046

COST REIMBURSEMENT TRAVEL, TOOLS and ODCs CLINs

CLIN	Description		Total NTE Price
4003	Long-Distance Travel Including G&A (b) (4)	NTE	$ 100,000
4004	Tools Including Indirect Handling Rate (b) (4)	NTE	$ 13,100,000
4005	ODCs Including Indirect Handling Rate (b) (4)	NTE	$ 0.00

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
4006	Contract Access Fee	NTE	$100,000

TOTAL CEILING FOURTH OPTION PERIOD CLINs: (b) (4)

GRAND TOTAL ALL CLINs: **$ 347,479,403**

B.5 SECTION B TABLES

B.5.1 INDIRECT/MATERIAL HANDLING RATE

Long-Distance Travel, Tools, and ODC costs incurred may be burdened with the contractor's indirect/material handling rate in accordance with the contractor's disclosed practices.

a. If no indirect/material handling rate is allowable in accordance with the contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on these costs.
b. If no rate is specified in the schedule of prices above, no indirect rate shall be applied to or reimbursed on these costs.

The indirect handling rate over the term of the TO shall not exceed the rate specified in the schedule of prices above.

B.5.2 DIRECT LABOR RATES

Labor categories proposed shall be mapped to existing Alliant labor categories.

B.5.3 INCREMENTAL FUNDING

B.5.3.1 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION

Incremental funding in the amount of $252,056,449.72 for CLINs 0001 through 3006 is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs may be allotted and available for payment by the Government as the funds become available. The estimated period of performance covered by the allotments for the mandatory CLINs is from award through January 18, 2021. The TO may be modified to add funds incrementally up to the maximum of $282,262,840 over the performance period of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

Incremental Funding Chart for CPAF

See **Section J, Attachment H** - Incremental Funding Chart (Excel Spreadsheet).

B.6 AWARD FEE PLANNED VALUE/RESULTS REPORTING TABLE

The Award Fee Determination Plan (AFDP) establishes award fee. See **Section J, Attachment I** – Award Fee Determination Plan (Word document).

C.1 BACKGROUND

The Department of Defense Cyber Crime Center (DC3) was unofficially formed in 1998 as an entity under the Department of the Air Force (AF). The initial operational capability brought together the Defense Computer Forensics Laboratory (DC3/CFL) and the Defense Computer Investigations Training Program (DCITP). DC3 is now designated as a National Cyber Center by the National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 and a Department of Defense (DoD) Center of Excellence by DoD Directive (DoDD) 5505.13E with the mission to set the standards in digital and multimedia (D/MM) forensics, develop and deliver specialized cyber investigative training, and serve as a focal point for information sharing on cybersecurity (CS) matters across the DoD.

The Secretary of the AF serves as the DoD Executive Agent for these activities and the Inspector General of the United States (U.S.) AF provides overall program management.

C.1.1 DC3 MISSION AND ORGANIZATION

DC3's mission is to deliver superior D/MM lab services, cyber technical training, technical solutions development, and cyber analytics for the following DoD mission areas: information assurance (IA) and critical infrastructure protection (CIP), law enforcement and counterintelligence (LE/CI), document and media exploitation (DOMEX), and counterterrorism (CT).

Located in Linthicum, Maryland, DC3 components serve the DoD and other U.S. Federal agencies throughout the world. The DC3 organization consists of a mix of military, civilian, and contractor support personnel. The DC3 environment is dynamic and constantly evolving which contributes to priorities frequently changing.

DC3 is operationally aligned into the organizations described below each with interrelated missions and support requirements that collectively contribute to the overall mission.

The DC3 is comprised of five operational directorates and two support directorates:

Operational

a. Computer Forensics Laboratory (DC3/CFL)
b. Technical Solutions Development (DC3/TSD)
c. Cyber Investigations Training Academy (DC3/CITA)
d. Defense Industrial Base Collaborative Information Sharing Environment (DC3/DCISE)
e. Cyber Crime Center – Analytical Group (DC3-AG)

Support:

a. Business and Technology Operations (DC3/BTO)

Computer Forensics Laboratory (DC3/CFL)

DC3's DC3/CFL performs D/MM forensic examinations, device repair, data extraction, and expert testimony for DoD. The lab's robust intrusion and malware analysis capability supports other DC3 lines of business and activities.

DC3/CFL operations are accredited under International Organization for Standardization (ISO)

17025 by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) which guides reliable, repeatable, and valid exam results, subjected to quality control and peer review.

Technical Solutions Development (DC3/TSD)

DC3/TSD tailors software and system solutions engineered to the specific requirements of digital forensic examiners and cyber intrusion analysts. DC3/TSD validates commercial off-the-shelf (COTS), Government off-the-shelf (GOTS), and in-house developed software/hardware before it can be used in a forensic process. In addition, DC3/TSD functions as the DoD repository for cyber CI tools.

Cyber Investigations Training Academy (DC3/CITA)

DC3/CITA provides the state-of-the-art cyber investigative training to individuals and DoD elements whose responsibilities include ensuring DoD information systems are secure from unauthorized use, CI, and criminal and fraudulent activities.

Note: This acquisition will not provide direct contract support for the DC3/CITA mission. Contract support for the DC3/CITA is obtained via a separate TO.

DoD-Defense Industrial Base Collaborative Information Sharing Environment (DC3/DCISE) As the operational hub for the Defense Industrial Base (DIB) CS Program, DC3/DCISE assists DIB companies to safeguard DoD content and intellectual property residing on or transiting their unclassified networks. DC3/DCISE develops and shares actionable threat products, and performs cyber analysis, diagnostics, and remediation consults for DIB Partners.

DC3/DCISE is the reporting and analysis center for the implementation of the statutory requirement in Section 941 of the Fiscal Year (FY) 2013 National Defense Authorization Act for reporting cyber incidents by Cleared Defense Contractors (CDCs), and the related amendment of the Defense Federal Acquisitions Regulation Supplement (DFARS), known as "Safeguarding DFARS."

Cyber Crime Center Analytical Group (DC3-AG)

AG performs technical analyses supporting the investigations and operations of national LE/CI agencies. The primary agencies served are the Air Force Office of Special Investigations (AFOSI), Naval Criminal Investigative Service (NCIS) and the Federal Bureau of Investigation (FBI).

DC3-AG is also a member agency of the National Cyber Investigative Joint Task Force (NCIJTF) and leads collaborative analytical and technical exchanges with subject matter experts (SMEs) from LE/CI, Computer Network Defense (CND), United States Intelligence Community (USIC), and IA agencies. The purpose of these information exchanges is to enable proactive LE/CI cyber operations.

Vulnerability Disclosure Program (DC3/VDP)

The Office of Under Secretary of Defense for Policy, the Office of the DoD Chief Information Officer, and U.S. Cyber Command, the DoD Voluntary Disclosure Program (DVDP) achieved initial operational capability on 21 November 2016. The DVDP implements the new Vulnerability Disclosure Policy approved by the Secretary of Defense and the Department of

Justice which authorizes private-sector cybersecurity researchers (AKA Hackers) to scan public-facing DoD web sites for vulnerabilities.

DC3 is the sole focal point for receiving vulnerability reports and interacting with researchers. DC3 ensures that reports are delivered to the system owner and remediation personnel as quickly as possible

Business and Technology Operations (DC3/BTO)

BTO is the support element of DC3 and provides strategic planning, resource programming and management, portfolio management, information management, policy development, administration workforce, technology, security, and resource solutions that enable operations in a complex dynamic cyber environment. BTO consists of seven functions: human resources, security administration, financial management, contract administration, information management/information technology (IT), CS, and logistics.

C.2 SCOPE

The scope of this effort is to provide technical and functional support to DC3 operational and support directorates. The support includes program management, DC3 operational support, D/MM forensic technician and examination support, software development, IT infrastructure, network and CS, cyber threat analysis, and surge support.

The primary place of performance is onsite at DC3's facilities in Linthicum, MD. The secondary sites include National Media Exploitation Center (NMEC) in Northern Virginia, the NCIJTF in Chantilly, Virginia (VA) and the DIB in Alexandria, VA. Performance at off-site locations is only permissible in rare cases and shall be approved in advance by the TPOC.

Long distance travel is required within the Continental United States (CONUS) and Outside Continental United States (OCONUS) to provide support to the DC3 mission, to include training, conferences/seminars/workshops, technical briefings, evidence examination, and testimony in military courts martial or other state, Federal, local, or tribal court associated to digital forensic exam conducted by examiner.

C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

DC3's IT services are maintained in accordance with all DoD and AF directives, guidelines, and requirements such as (but not limited to) DoDD 8570, AF Manual (AFMAN) 33-285 and AFMAN 33-282.

DC3 operates and maintains one Non-classified Internet Protocol (IP) Routing Network (NIPRNET), one Secret Internet Protocol Routing Network (SIPRNET) network, one Joint Worldwide Intelligence Communications System (JWICS) and multiple stand-alone forensic/examination networks that provide processing and communications support.

The NIPRNET provides seamless interoperability for unclassified combat support applications, as well as controlled access to the Internet. SIPRNET is DoD's largest interoperable command and control data network, supporting the Global Command and Control System (GCCS), the Defense Message System (DMS), collective planning, and numerous other classified warfighter applications.

Over the life of this task order, the Government will be transitioning ITD to the latest Information Technology Infrastructure Library (ITIL) framework for IT Services Management (ITSM). The contractor shall be responsible for implementing, transitioning and maintaining ITD operations using the ITIL framework.

C.4 TASKS

C.4.1 TASK 1 – ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the DC3 via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil/.

Reporting inputs will be for the labor executed during the period of performance during each Government FY, which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year.

Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure web site without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

C.4.2 TASK 2 – PROGRAM MANAGEMENT

The contractor shall provide on-site program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS). The contractor shall identify a Program Manager (PM) by name that shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

C.4.2.1 SUBTASK 1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at the location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor personnel, representatives from the DC3 Directorates, other relevant Government personnel, and the Federal Systems Integration Management Center (FEDSIM) Contracting Officer's Representative (COR). The contractor shall provide the following at the Kick-Off Meeting:

a. Updated Transition-In Plan **(Section F, Deliverable 03)**
b. Updated Quality Control Plan (QCP) **(Section F, Deliverable 08)**

C.4.2.2 SUBTASK 2 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an MSR (Section J, Attachment B) within five business days after the Technical Status Meeting (TSM), or upon Government direction if TSM is cancelled via electronic mail (email) to the Technical Point of Contact (TPOC), CO and the COR (Section F, Deliverable 09).

At a minimum, the MSR shall include:

a. Quantifiable work performed during the reporting period. This data shall be aligned to the tasks set out in this TO and describe the work done; the labor hours associated with that effort, and measured outcomes.
b. Areas of concern and/or problems identified and any Government actions required to facilitate the remediation of these identified issues.
c. Personnel gains and losses per task area.
d. Summary of any trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).
e. Detailed cost per CLIN and WBS Element as defined by the Government clearly showing the aggregated hours of contractor work invoiced and the specific TO area for which that effort was expended.
f. Projected costs of each CLIN and WBS Element as defined by the Government for the forecasted duration of each WBS element starting with month-end June 2018 data
g. Other specified deliverable information.

C.4.2.3 SUBTASK 3 – CONVENE TECHNICAL STATUS MEETINGS

The contractor PM shall convene a monthly Technical Status Meeting with the TPOC, COR, and other Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and the information provided in the MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR, CO and TPOC within five workdays following the meeting (Section F, Deliverable 66).

C.4.2.4 SUBTASK 4 – PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP. The PMP shall:

a. Conform to PMI best practices and methodologies.
    1. Include milestones, tasks, and subtasks required in this TO.
    2. Provide for an overall Work Breakdown Structure (WBS) and clearly identify contractor work efforts, responsibilities, and deliverables in support of that activity.
b. Clearly describe and define the contractor's management approach and its alignment to item (a).
c. Align all contractor work efforts to TO areas and requirements, and clearly demonstrate the level of effort requisite to completion of work in that task area.
d. Include the contractor's Quality Control Plan (QCP).

(Note: the PMP shall delineate between any work effort, support, contribution, or collaborative effort that is assisted by a Government employee.)

The contractor shall provide the Government with a draft PMP **(Section F, Deliverable 05)** on which the Government will make comments. The final PMP **(Section F, Deliverable 06)** shall incorporate the Government's comments.

The contractor's PMP shall be made available through the DC3 Information Center (IC) (Section C.4.4.6) and shall be updated regularly and maintained to reflect current operations.

C.4.2.5 SUBTASK 5 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted. The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and point of contact (POC) at travel location.

C.4.2.6 SUBTASK 6 – UPDATE THE QUALITY CONTROL PLAN (QCP)

The contractor shall update the QCP submitted with its proposal and provide an updated QCP **(Section F, Deliverable 08)** at the Kick-Off Meeting. The contractor shall periodically update the QCP as required in Section F, as changes in program processes are identified.

The QCP shall include:

a. The QCP shall delineate the contractor's contribution on work products and work efforts from the Government.
b. A full, complete and clear description of the inspection and monitoring systems used to cover all performance areas set forth in this TO.
    1. Specific areas inspected and contractor personnel performing work in support of the area inspected.
    2. Schedule / Frequency of Inspection
    3. Inspection format and deliverables
c. A description of the methods the contractor shall use for identifying, reporting, and preventing defects in the quality of work performed by contractor staff supporting this TO.
d. How the contractor shall maintain on-site records of all quality control inspections conducted by contractor personnel. Records shall include the name of the inspector, date of inspection, what was inspected, discrepancies found, corrective actions taken, date actions taken, date Government was notified, and name of Government official notified. The contractor shall keep documentation and make it available to the Government through the DC3 IC throughout the entire period of contract performance and for the period after contract completion until final settlement of all claims, if any, under the contract.

C.4.3 TASK 3 - BUSINESS AND TECHNOLOGY OPERATIONS (BTO)

The contractor shall support the BTO by providing administrative support, security, logistics, financial management, contract administration, human resources, information management, facilities, and IT services. These shared services enable each of the Directorates to focus on

delivery of their core mission and maintain a common operational support mechanism.

C.4.3.1 SUBTASK 1 – DC3 DIRECTORATE ADMINISTRATIVE SUPPORT

The contractor shall provide administrative support for DC3 and subordinate operational directorates. The contractor shall support handling incoming inquiries via email and telephone; coordinating and updating directorate calendars and project schedules; coordinating DC3 site visits, tours, and vendor demonstrations; maintaining office visit logs; and coordinating travel and security documentation.

Additionally, the contractor shall support customer processing requests/submissions and assist in project status tracking. Activities include updating Directorate-specific databases such as project management software, case management systems, and knowledge management portals.

The contractor shall develop and maintain standard operating procedures (SOPs) for all activities performed on behalf of administrative function **(Section F, Deliverable 10).** The contractor shall produce weekly activity reports (WARs) for appropriate Directorate leadership.

C.4.3.2 SUBTASK 2 – DC3 PLANNING, PROGRAMMING, EXECUTION, AND BUDGET SUPPORT

The contractor shall provide assistance to the DC3 BTO in preparing strategic planning, resource programming and management, portfolio management, information management, and policy development and administration.

Strategic Planning and Policy Development

The contractor shall provide IT policy and planning expertise to perform DC3 program planning, financial management, and analysis for complex cyber programs. The support requires extensive operational and financial coordination with other National, DoD and AF IT programs. Programs relate to one or more of the following strategic or operational areas: cyber training (DC3/CITA), cyber forensic capability development, D/MM forensic examinations, cyber investigations and operations, cyber threat analysis, and the DIB CS.

The contractor shall support continual assessment and interpretation of National, DoD, and AF strategies and guidance for application to DC3 missions through development of organizational strategies and implementing policies. The contractor shall consult and coordinate with staff from other DoD organizations and Federal agencies to interpret, develop, and modify strategies and policies to ensure efforts meet program needs. The contractor shall keep abreast of changes in policy direction and assesses impact on DC3 mission requirements. The contractor shall present findings to DC3 leadership and make recommendations for improvement where appropriate. The contractor shall assist DC3 with the development and sustainment of the organizational Strategic Plan and implementing policy documents; development and sustainment of the DC3 performance measurement program; as well as the development, implementation, and management of process improvement plans.

Resource Programming and Management

The contractor shall research, analyze, collate, and evaluate data from existing manpower and budgetary databases (i.e., Automated Budget Interactive Data Environmental System (ABIDES), intelink Resource Management Information System (iRMIS) etc.), Congressional Records, DoD, U.S. Unified and Specified Commands, and AF operational commands to develop optimum

investment strategies. The contractor shall assist in the formulation of and monitor the execution of long-range detailed budget forecasts, financial plans, and five-year programs to fund implementation of substantive cyber programs and projects. The contractor shall conduct detailed research of budget forecasts and execution histories from a number of highly technical cyber programs to identify trends, anomalies, and potential capability gaps. The contractor shall analyze guidance for multi-year appropriations to identify resource shortfalls and offsets, prepare appropriate supporting documentation, and identify alternative methods of financing unfunded requirements. The contractor shall maintain DC3 information in manpower, programming, and budgeting databases as well as providing timely and accurate response to inquiries and taskings pertaining to DC3 planning, programming, and budgeting.

The contractor shall coordinate on and prepare responses to mission-related administrative taskings from the Executive Director of DC3 and higher echelons. This includes staffing taskings with appropriate DC3 Directorates; evaluating, deconflicting, and aggregating inputs received; analyzing facts, performing appropriate research, and applying functional expertise to prepare recommended responses for DC3 leadership (e.g., DC3 coordinated and prepared responses to over 60 mission-related administrative taskings in Calendar Year (CY) 2015). The contractor shall provide timely and accurate development of staff packages, staff studies, and papers in accordance with AF Handbook 33-337, The Tongue and Quill.

DC3 currently manages 54 Cooperative Research and Development Agreements and 40 other support agreements. Agreements are reviewed, revised, and/or terminated on an annual basis. Six new Cooperative Research and Development Agreements and six new support agreements were initiated in CY2015. In support of these efforts, the contractor shall develop, coordinate, and maintain agreements between DC3 leadership and external organizations. This includes Cooperative Research and Development agreements supporting educational partnerships and transfers of technology as well as other mutual support agreements. Efforts entail clarifying and documenting requirements and expectations of all parties to the agreement and ensuring resource implications are properly addressed. The contractor shall provide timely development of Memorandums of Agreement, Memorandums of Understanding and Support Agreements in accordance with DoDD 4000.19 and Air Force Instruction (AFI) 25-201; and the timely development of Cooperative Research and Development Agreements in accordance with DoDD 5535.3, DoD Instruction (DoDI) 5535.8, and AFI 61-301 and 61-302.

Portfolio Management

The contractor shall assist the BTO in establishing a DC3 Portfolio Management (PfM) capability to centralize management of all DC3 portfolios (directorates). For example, the developed ITD portfolio will ensure systematic management of IT investments, projects, and activities. The capability shall assist BTO portfolio managers in identifying, prioritizing, authorizing, managing, and controlling projects, programs, and other related work within the DC3 directorates to achieve DC3 strategic business objectives. Additionally, the DC3 PfM will include a subset capability of Project Portfolio Management (PPM) to standardize project processes, methods, and technologies used by project managers and project management offices (PMOs) throughout DC3. The capability will allow the portfolio manager to analyze and collectively manage current or proposed projects. The desired capability will allow for effective requirements prioritization based on mission needs and mapped to budget resources.

Mission Partner Liaison Support

The contractor shall support efforts as a liaison with other DoD organizations and Federal agencies to integrate DC3 policy, planning, and resource actions. This includes promoting the exchange of information on requirements, capabilities, deficiencies, as well as emerging technologies and cyber threats. The contractor shall assist DC3 leadership with presenting, justifying, and defending DC3 positions on issues of considerable consequence and importance. The contractor shall work collaboratively with external mission partners to achieve common understanding and reasonable resolution of controversial issues. The contractor shall coordinate efforts to minimize operational conflicts and/or duplication in order to best achieve overall DoD and National strategies related to core DC3 cyber missions. In support of these efforts, DC3 regularly hosts and attends planning meetings with external mission partners to include Federal Cyber Centers, LE, Intelligence Community, and DoD. The meeting topics cover a broad scope of mission-related activities including training, Forensic Examinations, Forensic Tool Development, LE/CI Threat Analysis, and DIB CS support. On average, the meetings consist of in-person meetings approximately once a week at a minimum. As such, the contractor shall facilitate and/or attend meetings, forums, working group sessions, and conferences; develop and present informational briefings; develop and/or analyze read-ahead material; provide historical records; and document and analyze results from such sessions.

Information Management

The contractor shall assist in developing, implementing, and maintaining an information management (IM) capability. The IM capability shall address enterprise-wide DC3 electronic and records management systems (includes knowledge management system) and establish standardized IM practices, ontologies, taxonomies, meta-data tagging schemas, and management controls in support of DC3 document and record systems, including classification, retrieval and retention processes. The IM capability shall address acquisition of information from one or more sources, the custodianship and the distribution of that information, and disposition of it through archiving or deletion. The IM capability must address the accounting and administration of digital content throughout its lifecycle, from creation to permanent storage or deletion. The digital content will consist of images, video, audio and multimedia, as well as text. The contractor shall develop and document IM standards, ontology, and taxonomies for lifecycle management and records management of information and data acquired, processed, used, stored, and disposed by the DC3. The contractor shall document and maintain the IM SOPs **(Section F, Deliverable 16)**.

C.4.3.3 SUBTASK 3 – DC3 OPERATIONAL SECURITY

The contractor shall assist the Government security manager in supporting the continuous maintenance of DC3's physical information and personnel security program in accordance with AF and DoD policies and regulations. DC3 currently uses e-QIP, Scattered Castles, and the Joint Personnel Adjudication System (JPAS) for personnel security processing. Security personnel supporting this contract are required to possess a Top Secret (TS) Sensitive Compartmented Information (SCI) clearance in order to obtain a JWICS account for communicating on sensitive security matters (e.g., Sensitive Compartmented Information Facility (SCIF) accreditation/re-accreditation packages.)

The contractor shall work with DC3's security office to ensure the physical security of DC3 facilities (currently located in DC3 buildings 911, 1190, and 1306), ensure classified information is handled and discarded in accordance with DoD policy, manage DC3's SCIFs, manage

personnel clearances, maintain access controls to DC3 facilities, and other security related functions. The contractor shall provide support for facility alarm systems, closed circuit television (CCTV) controls, access control methods and emergency response procedures, and conduct security surveys and assessments.

C.4.3.4 SUBTASK 4 – DC3 PURCHASING AND SUPPLY MANAGEMENT

The contractor shall provide standard supply chain management support to include requirements determination, purchasing, asset receipt and management, inventory control and accountability, and vehicle management functions to DC3's logistics (LG) support office. This shall include, but is not limited to, implementing and sustaining DC3's material and equipment inventories, asset receipt and disposal, routine and large purchasing actions, vehicle fleet management, mail room services, and other logistics functions.

DC3 currently utilizes a self-service SharePoint capability for vehicle fleet management. The Government intends to move this capability into Footprints application in order to centralize the management and metrics of vehicle use. The capability will continue to support self-service as well as tracking of administrative functions, such as vehicle checks, fluid level checks, and condition reporting, and form automation capabilities.

The contractor shall also support DC3 contracting procurement requirements by researching alternatives to asset requisitioning; timely input of requisitions in accordance with supporting contracting office and FAR; coordination with supporting Government Purchase Card (GPC) program and large purchase contract offices (i.e., 11 CONS, AFDW/PK, GSA FEDSIM, etc.); and tracking orders to receipt, formal issue of items to end user, full accountability of assets in use, and proper disposal of assets at life cycle end.

The contractor shall perform all support in accordance with DoD guidance and AF policies and regulations.

C.4.3.5 SUBTASK 5 – HUMAN RESOURCES MANAGEMENT

The contractor shall assist DC3's Human Resource Management with administrative functions such as maintaining and generating reports and metrics, execution of personnel actions, and other human resource management activities. The contractor shall stay abreast of the latest AF and DoD guidance and policies, and perform work in accordance with the latest policies and procedures. The contractor shall track the execution of DC3 personnel actions, provide analysis of HR guidance, and provide full spectrum management and reporting of DC3's HR program.

Additionally, the contractor shall assist in developing a comprehensive workforce and talent management plan and program for improving the current workforce, and assuring DC3 maintains a competitive, well-trained, robust talent pool.

C.4.3.6 SUBTASK 6 – DC3 FACILITIES MANAGEMENT

The contractor shall support DC3's facilities and infrastructure program in accordance with AF and DoD policies and regulations. The contractor support shall include but is not limited to maintaining and generating reports and metrics, assisting in the execution of real property related activities, tracking of facilities projects, and other facilities management and infrastructure activities. The contractor shall assist in functions to support a Military Construction (MILCON) project. The contractor shall maintain a DC3 seat allocation that captures the specific location of

individuals within DC3 areas.

The contractor shall manage DC3's facilities help desk ticketing system (currently Footprints). The contractor shall provide responsive and timely resolution for facilities-related issues.

The contractor shall ensure all facilities issues and incidents are recorded and reported monthly, appropriate metrics are maintained, and that these metrics are made available to the Government via the DC3 IC.

C.4.3.7 SUBTASK 7 – DC3 COMMUNICATIONS SUPPORT

The contractor shall support strategic and tactical communication efforts to enhance DC3's internal and external messaging and outreach. The support includes a variety of ad-hoc projects in digital communications, marketing, graphics, and general outreach support for the DC3 organization. The contractor shall also assist in establishing communications standards for various communications channels, such as, web services, publications, presentations, and etc. The contractor shall establish a consistency for branding, customer engagement, and reduction of duplication or disparate information management artifacts.

The contractor shall support the DC3 Dispatch (e.g., news and informational emails sent to internal and external recipients). The contractor shall produce and distribute weekly DC3 news material and quarterly newsletters. The contractor shall create, distribute, and store DC3 physical and virtual media artifacts as required. The contractor shall update and maintain the operating procedures for all outreach communications activities.

Additionally, the contractor shall coordinate all press and media activity-related requests at DC3; all media requests with appropriate Public Affairs Office; all visitors and tours of DC3; and all DC3 briefings and speaker engagements as required.

The contractor shall provide photography and graphics support for DC3 to include, Multimedia Production (animations), Physical Media Production (compact discs (CDs)/digital video discs (DVDs)), DC3 logos, artwork, flyers, and brochures.

The contractor shall assist in establishing communications standards for various communications channels, such as, web services, publications, presentations, etc. The desired outcome is consistency of branding, customer engagement, and reduction of duplication or disparate information management artifacts.

C.4.3.8 SUBTASK 8 – DC3 TRAINING MANAGEMENT SUPPORT

The contractor shall develop, implement, and maintain a DC3-wide training management program to centrally manage all training requirements on behalf of DC3 personnel. The program shall be a support mechanism for acquiring, coordinating, and tracking DC3 training requirements as well as maintaining compliance with DoD/USAF personnel certifications and training. The training requirements primarily consist of external (third-party vendor) training and distance learning requirements.

The contractor is required to successfully complete and/or attend training identified by the Government. This training includes, but is not limited to: Information Assurance (IA) and Active Shooter.

The contractor shall collect training requirements from DC3 Directorates to develop an annual forecast aligned with the training budget in coordination with DC3 Financial Management. The contractor shall maintain an organization wide master folder tracking all DC3 personnel, including pertinent training information such as training requests, training purchases, certifications obtained, and compliance requirements.

The contractor shall coordinate and schedule requests for training (currently requests are made in a centralized portal via SharePoint) with individual DC3 personnel and external training vendors. The contractor shall maintain a public training calendar via web channels (i.e., SharePoint). The contractor shall coordinate training purchases with the GPC Holder. The contractor shall identify opportunities for bulk training requirements to maximize staff participation that increase Government efficiencies and cost savings.

The contractor shall provide a Monthly Status Report on personnel training management efforts to include personnel compliance, training requests, training schedule, and budget updates. The contractor shall develop and maintain DC3 Training Policy and Procedures **(Section F, Deliverable 22)**.

C.4.4 TASK 4 – INFORMATION TECHNOLOGY DIVISION (ITD) OPERATIONS SUPPORT

The contractor shall provide assistance to the ITD in support of DC3's IT infrastructure, help desk, and telecommunications requirements.

The ITD requires on-call contractor support to maintain 24 hours per day, seven days per week, 365 days per year (24x7x365) operational availability of critical networks and systems. The ITD is currently responsible for 12 separate networks and telecommunications systems of all classification levels serving more than 400 users throughout the DC3 organization. ITD critical networks and systems currently consist of the Unclassified DC3 Enterprise Network (DEN), Classified Secure DC3 Enterprise Network (SDEN), DC3's Open Network (DC3ON), DC3/CFL Networks (ExLAN, IA LAN), and phone systems. The ITD also maintains and supports all Corporate and Forensics applications that run on forensically sound workstations, several of which are mission critical.

Over the life of this task order, ITD will be transitioning to the latest Information Technology Infrastructure Library (ITIL) framework for IT Services Management (ITSM). The contractor shall be responsible for implementing, transitioning and maintaining ITD operations using the ITIL framework.

C.4.4.1 SUBTASK 1 – HELP DESK SUPPORT

The ITD Help Desk is the single POC for all DC3 computer user and telecommunications-related issues. The Help Desk supports the three primary Linthicum, Maryland locations. In 2015, the help desk received 4,100 calls/ requests via the Help Desk Ticket reporting system for assistance. The requests are generally resolved via first call resolution; however, technicians may be required to be dispatched to troubleshoot and provide immediate resolution to the problem. The issues occur based on various security classifications levels to include: Sensitive-but-unclassified (SBU), Secret, TS, SCI, Special Access Program (SAP) and Special Access Required (SAR). All technicians performing network functions (as defined in AFMAN 33-285 or later version) shall be Information Assurance Technical (IAT) level II or higher certified in accordance with DoDD

8570.01 and 8140.01.

The contractor shall provide Tier 0 (self-service), Tier 1 and 2 help desk support for all DC3 computer users. This activity includes requests for installation, repairs, and upgrades of existing equipment. The contractor shall provide personnel onsite daily to respond to technical support issues from 0600 - 1800 Eastern Standard Time (EST) on 12 hours a day, five days a week basis. The contractor is required to provide on-call support (outside of the standard working hours) for unplanned events. The contractor is required to adhere to the on-call support timelines defined per the service level agreements (SLAs).

The contractor shall develop the Tier 0 or self-service mechanism to support DC3 computer users. The contractor shall provide a technical Tier 1 help desk (initial caller support) for DC3. Tier 1 is the first point of customer contact for network related operational issues. Typical Tier 1 support includes, but is not limited to, requests related to COTS hardware failures, software failures, application questions, installations, relocations, turn-ins, access rights, hardware/software loaners, network communication failures, new user requirements, temporary computer product check-outs, and other computer related requirements. All issues beyond the capabilities of Tier 1 caller support are escalated to Tier 2 or Tier 3.

The contractor shall provide Tier 2 help desk technical support for DC3 user issues. The contractor shall serve as the SME for troubleshooting desktop support related issues. The contractor shall design, troubleshoot, and implement DC3 computer-related equipment. In addition to Tier 2 troubleshooting, the contractor shall:

a. Identify network problems due to design and implementation constraints.
b. Identify and implement workarounds to resolve DC3 network problems.
c. Work with DC3 network design engineers on engineering and design issues to develop operationally sound implementations.
d. Develop troubleshooting guides and SOPs to improve Tier 0 and enable Tier 1 technicians to efficiently troubleshoot and resolve DC3 network problems.

The contractor shall respond to and document all network incidents including security and informational requests that result from proactive network monitoring or customer-initiated contacts. The contractor shall isolate and document network problems using industry best practice troubleshooting skills, as well as available system and network management tools. The contractor shall use the Help Desk Ticket application (currently Footprints) as a central repository for technical advice and solutions for network systems, software applications assistance, automatic data processing support, hardware exchange, and repair service support.

The contractor shall utilize network management tools to provide efficient, responsive, and rapid problem resolution.

The contractor shall collect and report IT help desk service performance metrics. The contractor, as a minimum, shall establish and maintain metrics (subject to Government approval) of the following items, and be prepared to present the findings to DC3 management:

a. Total number of queries into the ITD
b. Total number of queries into the ITD that result in a trouble ticket (separated by category, such as, incidents, problems, requests for change, and requests for services)
c. Total number of queries that are resolved during initial contact

d. Total number of queries resolved by the ITD
e. Total time to complete (resolve) the trouble ticket

The contractor shall adhere to the approved SLA process for responding to help desk queries. At a minimum, the contractor shall respond to customer help desk requests within four hours and complete resolution within 24 hours (during regular business hours M-F 0600 - 1800 EST). The contractor shall provide supporting documentation to be validated by the DC3 TPOC for those requests beyond the desired response and resolution periods. The contractor shall track all help desk requests through to completion in the help desk ticketing system.

The contractor shall provide Monthly Help Desk Trouble Call Status Reports (TCSRs)**.** The contractor shall provide Help Desk TCSRs that provide relevant data and reports on information such as:

a. Analyses/type of trouble calls
b. Unusual patterns
c. Potential DC3 IT/Communications/application problems and proposed resolutions
d. Unresolved Trouble Tickets
e. Tracking and resolution of service complaints
f. Backup source data
g. Summary status (in spreadsheet format) of all hardware maintenance for each month

C.4.4.2 SUBTASK 2 – NETWORK AND SYSTEMS ADMINISTRATION SUPPORT

DC3 relies upon the following networks (currently 12 in total) and their associated services for its daily operations and mission support:

a. DC3 Enterprise Network (DEN) NIPRNet (supporting approximately 450 users)
b. Secure DC3 Enterprise Network (SDEN) SIPRNet (supporting approximately 250 users)
c. Joint World-Wide Communications System (JWICS) (supporting approximately 200 users)
d. DC3’s (internal) Laboratory Information Management System (CIMS10), Forensic Examiner, and Intrusion Networks
e. DC3's Open Network (DC3ON)
f. Covered Accounts Network
g. Virtual Private Network (VPN) on unclassified networks
h. Other networks as required by the Government (e.g., Defense Industrial Base LAN (DIBLAN))

The contractor shall ensure identified networks (currently DEN, SDEN, DC3ON, and DIBLAN) align to the complete Risk Management Framework (RMF) and successfully obtain and maintain Authority to Operate (ATO).

The contractor shall install and maintain routers, switches, hubs, and cabling comprising DC3’s networks. The contractor shall maintain the IP addressing schema for the entire enterprise infrastructure; modify switch, router, and hub configurations to ensure optimum network performance; and configure Access Control Lists (ACLs) to grant/restrict network access to

authorized uses and protocols.

The contractor shall provide proactive and reactive management of resources by monitoring and controlling networks, available bandwidth, hardware, and distributed software resources.

The contractor shall operate and maintain the aforementioned networks to include but not limited to the following tasks:

a. Install, configure, manage, troubleshoot, and secure network infrastructure, including but not limited to servers, storage components, desktop computers (PCs), laptops, printers, scanners, routers, switches, network devices, and other tools.
b. Design and configure network components, including VPN capabilities.
c. Monitor and manage network bandwidth.
d. Perform back-up and recovery functions.
e. Establish, monitor, and maintain all computer and network accounts (Add/Change/Deletion) in accordance with DoD, AF and DC3 BTO/ITD computer security regulations.
f. Maintain the Global Address List, MS Active Directory and other network directory services.
g. Maintain an up-to-date listing of user accounts, email accounts, passwords, software licenses, systems file directories, and system/network accreditation documentation.
h. Operate, maintain, and trouble-shoot video teleconferencing hardware and software
i. Manage internet and intranet web servers, remote Access Security Services, and maintain the Domain Name System (DNS) server.
j. Maintain and monitor standardized file storage directory structures.
k. Establish, maintain, and monitor print servers.
l. Coordinate with third party organizations and network carriers to perform operational activities.
m. Develop and document network administration policies and procedures.
n. Document and report all network faults, outages, and security incidents**.**
o. Document and maintain enterprise user account information.
p. Conduct analysis of network characteristics to include traffic, connect time, transmission speeds, packet, and modifications to network and system components.
q. Recommend processes and tools to improve overall network performance and user experience.

All technicians performing network functions (as defined in AFMAN 33-285 or later version) shall be, at a minimum, IAT level II certified in accordance with DoD 8570.01 and DoD 8140.01.

Over the performance period of this TO, the DC3 desires to move its existing infrastructure to a thin client environment. The contractor shall provide implementation and maintenance support for all new infrastructure changes or surge efforts as required.

The contractor shall also make recommendations to the Government for upgrades, equipment replacement, repairs, changes, additions, and removal of parts of DC3 IT infrastructure. The

contractor shall notify the Government of all necessary required changes, additions or removals from the existing system and obtain concurrence before any changes, additions, or removals are performed. The DC3 has a configuration control process to document and approve all changes to the IT services baseline. The contractor shall ensure all changes are processed through this process and conform to established policy and standards. The contractor shall document all repairs, changes, additions, or removals in the summary status included in the TCSR. The contractor shall conduct technical testing on existing and newly procured ITD systems, subsystems, and applications. The contractor shall evaluate communications hardware and software, troubleshoot problems, and provide technical expertise for optimal performance of equipment. The contractor shall recommend additional hardware and software tools which could improve the systems.

The contractor shall ensure that DC3's networks and systems shall maintain monthly 99.5 percent network/systems availability. The contractor shall notify the Government of any unusual circumstances that exist beyond the contractor's control for not meeting the availability service levels. The contractor is required to monitor, maintain, track, record, and report monthly system availability, up-time, and down-time. This information shall be made available, on-demand, to the Government via the DC3 IC.

In the event that network connectivity/availability is caused or impacted by an external source (not DC3), the contractor will ensure the BTO Director and TPOC are notified, in writing, within 30 minutes of the incident (during regular business hours M-F 0600 - 1800 EST). This report shall include the cause and anticipated restoration time.

The contractor will ensure all network incidents are identified in the MSR with descriptions of the incident, causes, resolutions, and any Government actions required. The contractor will ensure this information is made available, on demand, to the Government via the DC3 IC.

The contractor shall respond to detected security incidents, network faults (errors), and user reported outages within 30 minutes of notification of an incident. The contractor shall notify the Government (BTO Director, TPOC) within 30 minutes of any security incident or network outage (during regular business hours M-F 0600 - 1800 EST). The contractor shall document, record, and report all network incidents and include these within the MSR**.**

C.4.4.3 SUBTASK 3 – ENTERPRISE ARCHITECTURE (EA) AND CONFIGURATION MANAGEMENT (CM)

DC3's EA conforms to the DoD Joint Information Environment (JIE), which consists of five major focus areas: optimization of information, network, hardware, applications, and governance. Each of these capabilities is described in terms of activities, services, and rules necessary to ensure the capability is achieved. The DoD Information Environment Area (IEA) outlines how capabilities are delivered by providing descriptions of services the DoD IEA must have to operate at optimum effectiveness. These services represent a collection of required information across the spectrum of Doctrine, Organization, Training, Material, Leadership and education, Personnel, Facilities, and Policy (DOTMLPF-P).

The contractor shall develop and maintain the baseline artifacts of the following views: AV-1, AV-2, CV-1, CV-2, CV-6, CV-7, OV-1, OV-5a, OV-6a, SvcV-1, SvcV-4, StdV-1, and StdV-2.

Furthermore, the contractor shall provide documentation in accordance with DC3 standards to substantiate the DC3 current and future states as the DC3 architecture evolves **(Section F,**

Deliverable 26).

The contractor shall be responsible for requirements analysis, evaluation, and design of the IT architecture environment for DC3. The contractor shall maintain a current EA and configuration design for all DC3 networks. The contractor shall provide DC3 with a well-defined practice for conducting enterprise analysis, design, planning, and implementation, using a holistic approach at all times, for the successful development and execution of strategy. The contractor shall apply architecture principles and practices to guide the DC3 through the business, information, process, and technology changes necessary to execute its strategies and objectives.

The contractor shall develop, implement, and support DC3's Configuration Management (CM) processes for all networks and supporting technologies identified in this TO. The DC3 CM shall consist of a systems engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life. This shall include assurance of adequate software CM that tracks and controls changes in any DC3 software or application thereby maintaining strict accounting of the DC3 IT services baselines.

The CM system process shall include configuration identification, data management, audits, change control, status accounting, and deficiency reporting. The CM system/process shall be documented in a Configuration Management Plan (CMP) that includes/addresses the entire IT lifecycle.

The contractor shall support the installation and configuration of network servers, routers, and other peripherals. The contractor shall be responsible for CM design, architecture, and COTS/GOTS software and hardware integration to include, but not limited to, describing provisions for configuration identification, configuration of requirements documentation, design documentation, software, and related documentation.

The contractor shall be responsible for configuration change control, configuration status accounting, and configuration audits. The contractor shall regulate the change process so that only approved and validated changes are incorporated into product documents and related software. The contractor shall track and report all CM problems and support software quality assurance process audits.

The contractor shall evaluate, implement, and configure hardware and software to ensure Air Force Information Protection (AFIP) and DOD policies are enforced and safeguards are active.

The contractor shall configure test beds to conduct testing on DC3 networks; record and analyze results; and provide recommendations for improvements of the products/systems tested. The contractor shall encode, debug, and test software applications to meet established operational and system requirements using industry standard products such as programming languages and tools as required.

C.4.4.4 SUBTASK 4 – IT ASSET MANAGEMENT

The contractor shall provide support in receiving, tracking, distributing, and accounting for DC3's hardware and software inventory. DC3 currently utilizes Wasp asset management software.

The contractor shall maintain an up to date library of all major equipment warranty/maintenance contract information as well as life cycle end of life (EOL) status.

The contractor shall support maintaining a complete inventory of all of DC3's major hardware and/or designated components and the recording of serial numbers and related nomenclature. The contractor shall maintain and update a software library accounting for all software, licenses, and issuance data**.** The contractor shall ensure all asset lifecycle information is tracked, monitored, and reported appropriately to ensure timely renewal or refresh of end-of-life assets.

The contractor shall document and regularly update the total cost of operations (TCO) for each DC3 network in accordance to guidelines provided by the Government. The need to identify costs as well as provide investment transparency, the contractor shall assist the Government in developing a chargeback or show back model that depicts IT investments by identifying the components of IT costs that are directly associated to the infrastructure, data transfer, application licenses, training, etc., which they generate. The intent is to ensure appropriate use of IT resources, providing visibility to the DC3 leadership, substantiate rationale for IT decisions, and conform to budgeted IT services.

The contractor shall ensure IT asset information is made available to the Government, on demand via the DC3 IC.

C.4.4.5 SUBTASK 5 – CYBERSECURITY (CS)

The contractor shall assist in maintaining CS protection of all DC3 data and systems. The contractor shall provide technical support to maintain the confidentially, integrity, and privacy of DC3 mission information systems.

The contractor shall support the DC3 Chief Information Security Officer (CISO) in executing the CS requirements for DC3 information technologies through the use of the RMF consistent with the principles established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 and as outlined in DoDI 8510.01, RMF for DoD IT. The contractor shall perform continuous monitoring activity and support the implementation and operations of an insider threat capability**.** The contractor shall continually identify and inject RMF requirements into DC3 acquisition processes, requirements development, procurement, and IT (hardware and software) development efforts.

The contractor shall provide services to include active security vulnerability assessment, implementation, and monitoring of all computer systems and network infrastructure. The contractor shall perform vulnerability/risk analyses of computer/network systems and applications during all phases of the system development life cycle. The contractor shall assist in conducting certification and accreditation on applications in accordance with the RMF.

The contractor shall assist in eliminating the threat of network intrusions by proactively probing network defenses to identify vulnerabilities to include administering network scans as required.

The contractor shall ensure the latest security updates are enforced, ensure Information Assurance Vulnerability Alert (IAVA) and Tactical Computer Network Operator (TCNO) compliance, and provide real-time protection from any threats of active files using anti-virus tools. The contractor shall operate and maintain firewall(s), web proxy, caching servers, and e mail gateway servers to protect DC3 information resources from internal and external threats. The contractor shall ensure all current network security tools and patches are implemented across all internal DC3 systems in accordance with AF and DoD standards. The contractor shall conduct daily security scans of computer/network systems and advise the Government of potential computer security concerns and problems along with recommendations for solutions.

The contractor shall develop/maintain measures and controls to protect the DC3 networks from denial of service, unauthorized access, and modification of data and destruction of DC3 networks, network components, or information processed on them. The contractor shall document and maintain IT security policies, procedures and awareness.

The contractor shall perform information protection functions for networks and systems. The contractor shall test computer/network systems and applications for the following:

a. Ease of unregulated entry
b. Systems resources denial
c. System information corruption
d. Unlawful use of system resources
e. Vulnerability to electronic disruption

The contractor shall report and document all identified system attacks to the DC3 TPOC.

The contractor shall provide support related to Communications Security (COMSEC). The contractor shall document receipt, custody, issuance, transmittal, storage, accountability, classification, and destruction of all Classified Material. The contractor shall maintain logs and journals to comply with AF security, regulatory, and policy guidelines. The contractor shall be responsible for maintaining and updating all secure equipment, records, and self-inspection programs concerning Classified Material.

The contractor shall ensure all systems and equipment are operated and maintained in accordance with DoD, Defense Information Systems Agency (DISA), USAF, Secretary of the Air Force/Inspector General (SAF/IG) and AFOSI security guidelines, directives and updates. The contractor shall ensure all security policies are within the limits of existing architecture and software capabilities. The contractor shall ensure the DC3 network and systems are 100 percent in compliance with applicable DoD and USAF directives for Network and Computer Security.

C.4.4.6 SUBTASK 6 – DC3 INFORMATION CENTER (DC3 IC)

The Government is seeking a technical solution to collect, assess and make available to the Government metrics describing mission performance in all areas set forth in this TO. To that end, the contractor shall develop and maintain a secure, web-based (preferably located within DC3's NIPRnet) DC3 IC. The DC3 IC shall document DC3's operations, policies, procedures, program performance metrics, goals, and objectives. Formal approval of the design and specifications **(Section F, Deliverable 32)** will be conducted post-award. The initial operating capability of the DC3 IC shall be developed and implemented within six months **(Section F, Deliverable 33)** of formal approval and full operational capability within one year of formal approval **(Section F, Deliverable 34)**.

The DC3 IC shall have the technical capability to provide the Government and selected contract personnel program performance information to minimally include:

a. Dashboard - capable of providing at a glance summaries of operations, real time metrics (as set forth by the Government), and problem notifications.
b. Query - capable of providing the Government the ability to generate custom reports on program performance across DC3 directorates.
c. Resource management (to include financial resource management summaries),

procurement, IT lifecycle management, security, physical asset management, and facilities management.

The DC3 IC, at a minimum, shall address projects, processes, work flows, procedures, and associated performance metrics for DC3/CFL, DC3/TSD, DC3/DCISE, DC3-AG, and BTO directorates. All data tracked shall be clearly delineated between Government and contractor performed functions (e.g., personnel hours).

The DC3 IC shall have the technical capability of integrating and delivering the services currently available through DC3's internal portal (e.g., Help Desk System, Facilities Requests System, Vehicle Reservation System, Visit Request System, etc.).

The contractor shall ensure 100 percent compliance in accordance with AFI 33-114, Communications and Information Software Management.

C.4.4.7 SUBTASK 7 – WEB, PORTAL, AND CONTENT MANAGEMENT SYSTEM (CMS) DEVELOPMENT AND MANAGEMENT

The contractor shall support the DC3 internet and intranet websites, collaborative portals, and CMSs supported by this contract. The contractor shall provide administrative, development, and technical management of all facets of the managed websites, portals, and CMSs as directed by the responsible Government Information Management (IM) lead.

The contractor shall keep current all content on managed DC3 websites/portals and ensure these are compliant with DoD and USAF policies, directives, and standards. The contractor shall provide a review of all content updates at each MSR**.** The contractor shall perform continual evaluations of websites, portals, and CMS software and hardware to ensure continued and future effectiveness and efficiency of these capabilities and recommend updates, changes to the Government as appropriate and necessary.

The contractor shall design, develop and implement web pages that fully comply with AF/DOD/DC3 requirements and standards. The contractor shall maintain DC3's World Wide Web (WWW), NIPRNET, SIPRNET, DFI Portal and JWICS websites and content.

C.4.4.8 SUBTASK 8 – DATABASE MANAGEMENT SUPPORT

The contractor shall provide database installation, configuration and management for all DC3 databases. The maintenance of databases includes ensuring data reflected is accurate and current with incremental daily backups and a full backup provided weekly. The contractor shall modify the information contained in the database as directed by the Section Chief. The contractor shall ensure that information from the databases will be accessible to users as determined by the Section Chief using documented instructions provided by the contractor.

The contractor shall develop and administer security procedures to ensure only valid users have access to data and data modification. The contractor shall be responsible for ensuring data integrity while performing database related functions.

C.4.4.9 SUBTASK 9 – VIDEO AND TELECOMMUNICATIONS SUPPORT

The contractor shall provide overall support to DC3's telephone, telecommunications systems, and secure telecommunications equipment (currently Nortel and PBX). The contractor shall provide day-to-day technical administration of the phone system, perform scheduled and non-

scheduled maintenance, coordinate repair actions with service providers, and verify telecommunications circuits are active and available for use. The contractor shall monitor the performance of telephone sets, voicemail systems, modems, fiber optic cables, telephone switching units, and data circuits. The contractor shall provide immediate written notice within 24 hours to the DC3 ITD Director and TPOC of a situation impacting communications.

The contractor shall provide end-user training for telephone devices; configure voicemail, and all other phone system operations and features of the equipment.

The contractor shall provide onsite technical support for Audio Visual (AV) and Video Conferencing equipment (currently Tandberg) for multiple classification levels (NIPR, SIPR, and JWICS.)

C.4.5 TASK 5 – DEFENSE CYBER FORENSICS LAB (DC3/CFL) OPERATIONS SUPPORT

DC3 operates an ASCLD/LAB accredited digital data / multimedia forensic laboratory called the Defense Cyber Forensic Lab (DC3/CFL). DC3/CFL conducts examinations on digital and multimedia items submitted to the lab for analysis. DC3/CFL receives examination requests from all across the reach and scope of the DoD. DC3/CFL conducts a wide variety of examinations to include, but not limited to, homicide, child pornography, identity theft, counterfeiting, misconduct, terrorism, intrusions, fraud, and misuse of Government property. DC3/CFL operates across various security classifications levels to include: SBU, Secret, TS, SCI, SAP and SAR.

C.4.5.1 SUBTASK 1 - DC3/CFL INTAKE SUPPORT

The contractor shall support all lab inbound customer service inquiries. The contractor shall support review and validation of DC3/CFL forensic examination requests. The contractor shall support the lab with identifying potential conflicts with the operational workflow or policy impacts. The contractor shall recommend, update, and maintain the intake procedures; collaborate with the Director of Operations (DO); and identify forensic requirements of customer request and potential schedule.

C.4.5.2 SUBTASK 2 – DATA IMAGING AND EXTRACTION (I&E) SUPPORT

DC3 processes approximately 1,300 requests per year. Currently the average request is approximately 152 Gigabyte (GB) of data on 15 pieces of media. The contractor shall perform forensic imaging and extraction of digital information in support of examinations to develop evidence/intelligence information. The contractor shall ensure data imaging and extraction of media is completed within the defined timelines of the DC3/CFL (current estimate less than ten days.) The amount of time required is dependent upon the DC3/CFL complexity algorithm and determination of the DC3/CFL DO, Deputy Director, or Director. The size and complexity of each individual request is taken into consideration including the type, format, and condition of the media to be imaged in order to accurately estimate the reasonable suspense.

The contractor shall prepare and perform forensic imaging and extraction on computer digital devices and storage media such as hard drives, removable media, and optical removable media to include but not limited to:

a. Hard Disk Drives; floppy diskettes, ZIP drives, and similar removable disks
b. Data Tapes, Media Cards, Thumb Drives, CD ROMS, and DVDs

c. Smart Devices and Cell Phones
d. Digital Audio and Video Recording and Storage devices, Cameras, and Game boxes

The contractor shall be required, at times, to provide on-site imaging and extraction at specific evidence sites and alternate operating locations.

The contractor shall be responsible for extracting and duplicating forensically sound images of the media utilizing DC3/CFL-approved and specified imaging tools. Once the evidence or original media is extracted and duplicated, the contractor shall be responsible for archiving all image files to an appropriate storage media.

The contractor shall process forensically extracted data through Government provided software utilizing the hardware provided by the Government and approved SOPs.

The contractor shall record, document, and maintain written notes throughout the duplication process. The contractor shall process evidence and all associated corresponding administrative paperwork to include CIMS input and all other required forms in a proper and timely manner. The contractor shall document and report any noted evidence discrepancies. The contractor shall follow the procedures and methods outlined in the DC3/CFL SOP.

The contractor shall perform repair and recovery of data from damaged media on all cases assigned by the Government. The contractor shall employ specialized techniques for damaged media recovery, Hard Drive Repair, and CD/DVD ROM Disk resurfacing; and, produce restored copies of the suspect media for examination. Priority requests shall be determined based on the category or level involving national security or LE.

The contractor shall participate, present, and provide input at briefings, meetings, conferences, panels, boards, seminars, working group sessions, technical exchanges, and public forums on cyber-crime and forensic-related D/MM media imaging and extraction as needed.

C.4.5.3 SUBTASK 3 – EXAMINATION SUPPORT

The contractor shall support planning, organizing, and conducting digital media, forensic examinations of all items submitted to DC3 for analysis. The contractor shall support the examination of D/MM items submitted to DC3/CFL for examination in accordance with requirements set forth by the Government and Federal law, the Uniform Code of Military Justice, DC3 SOPs, DC3 Quality Assurance (QA) guidelines, and the DC3 Personnel Handbook.

The contractor shall conduct forensic analysis on items submitted to DC3/CFL for analysis, including but not limited to D/MM and audio/visual media cases to develop evidence/intelligence information in support of investigations. Cases shall be assigned by the Government.

The contractor shall conduct malware analysis, reverse engineering software development, and the cyber-attack lifecycle, from the initial exploit and malware execution path to callback destinations and follow-on binary download attempts.

The contractor shall provide a broad range of capabilities and skill sets to support D/MM forensics analysis, which includes but is not limited to:

a. Analyzing Large Data Sets
b. Loss of Control

c. Steganography
d. Global Positioning (GPS)
e. Peer-2-Peer Technologies
f. Cyber Malware Analysis
g. Malicious Code Analysis
h. Data Visualization/Data Mining
i. Metadata Retrieval/Analysis
j. Project Vision (Video and Image Retrieval/Analysis)
k. Public Key Infrastructure (PKI)
l. Biometrics
m. Encryption Detection and Defeat
n. Hard Drive Repair
o. Data Recovery from Damaged Advanced Media
p. Operating System (OS) Reconstruction
q. Password Cracking
r. Damage Assessment techniques along with GOTS and COTS software
s. Malware Analysis and Reverse Engineering
t. Cryptology

The forensic examination performed by the contractor shall normally include verification and comparison of the forensic image files; examination for the presence of malicious logic such as viruses, Trojans, worms, etc.; examination of media for deleted files and folders; documenting active and recovered deleted files; analysis for misnamed files; conducting word searches; and, analysis for relevant hardware and software configuration information.

The contractor shall assist in data recovery to determine the most appropriate method of protecting original evidence and recovering deleted, erased, hidden, and encrypted data.

The contractor shall write concise, comprehensive, and accurate notes throughout the examination process. The contractor shall develop a complete D/MM Forensic Analysis Report (DFAR) upon completion of the examination. The report shall be written in Microsoft Word (MS) (or appropriate) and document a complete examination. The contractor shall ensure the report is scientifically valid, readable, and compliant with all DC3 procedures.

The contractor shall perform technical peer reviews and feedback of other examiner cases. The technical peer review shall include reviewing other examiners reports for scientific validity, readability, and administrative compliance with all procedures.

The contractor shall be required to present findings of their examinations in Military, Federal, State, and/or local courts of law. The contractor shall provide expert/witness testimony of evidence findings, analysis, and examination. The contractor shall be prepared to provide forensic testimony on short notice requests. The contractor shall be required to travel to CONUS and OCONUS court proceedings to provide testimony.

The contractor shall assist the DC3 Attorney Adviser in providing technical reviews, analysis, and examination of all documents submitted and created by DC3/CFL regarding forensic

examinations. The contractor shall compare the information against the Fourth Amendment and Electronic Communication Privacy Act standards when making recommendations for disposition concerning forensic information and examinations.

The contractor shall assist the DC3 Attorney Adviser in preparing examiners for testimony in a court of law. The contractor shall develop charts and illustrations to support the DC3/CFL examiner in testimony at trial.

The contractor shall participate, present, and provide input at briefings, meetings, conferences, panels, boards, seminars, working group sessions, technical exchanges, and public forums on cyber-crime and D/MM forensic examination and analysis, as needed.

The contractor shall perform D/MM forensics examinations in support of the NMEC. This support includes processing critical national intelligence level cases that require expert analysis on audio/visual equipment, cell phones, and other mobile devices, and analyze information to determine useful data and content across a number of NMEC databases. The contractor shall perform audio and video forensics on commercial video systems and digital recording devices to extract, digitize, and enhance audio and video data for case agent review.

C.4.5.4 SUBTASK 4 – EVIDENCE CUSTODIAL SUPPORT

The contractor shall assist the evidence custodian in ensuring an effective evidence program is maintained and provides support services for all evidence entering and exiting DC3/CFL.

All contractor personnel assigned to the Evidence Room will be trained to handle evidence in accordance with DC3/CFL and DoD policies. Upon completion of the training program, personnel will be required to pass a written test to work in the Evidence Room.

The contractor shall receive, review, and maintain the integrity and proper custody of the evidence. The contractor shall identify and report any discrepancies in receipt of the evidence to the Evidence custodian**.** The contractor shall ensure forensic processes, handling, and hardware utilized are designed to safeguard all submitted evidence.

The contractor shall follow established procedures outlined in the ASCLD/LAB International Program (ISO 17025) Accreditation and AFOSI instructions for incoming evidence into the laboratory for media analysis. The contractor shall receive, inspect, and administratively process all incoming evidence, packages, and freight deliveries into the laboratory. Some items received may be large and the contractor shall be capable of handling heavy objects.

The contractor shall establish chain-of-custody document for all evidence to document the transfer of the evidence within DC3/CFL.

The contractor shall assist with logging in all evidence received by the DC3 in accordance with AFOSI evidence handling procedures and properly maintain the computerized evidence program. The contractor shall update and maintain the DC3/CFL Evidence Handling and Control Log and ensure it is current.

The contractor shall identify, photograph, store, and ensure all evidence is properly marked, tracked, and processed. The contractor shall update received evidence into the DC3/CFL Evidence Tracking System (ETS) and log new cases into CIMS.

The contractor shall seal and safeguard evidence and media in accordance with current DC3/CFL SOPs, ASCLD ISO 17025. The contractor shall assist in resolving evidence control problems.

The contractor shall create, update, and maintain case folders containing all required forms and supporting documentation for the case.

The contractor shall be responsible for issuing evidence to corresponding examiners. The contractor shall ensure the integrity of the evidence is maintained by ensuring all evidence is signed in and out. The contractor shall monitor and control the evidence in all aspects of laboratory operations and shall conduct reviews of all incoming and outgoing evidence chain-of-custody documents.

The contractor shall support a semi-annual inventory of maintained and stored evidence. The contractor shall document all stored evidence and verify evidence is logged into the ETS.

The contractor shall be responsible for returning all evidence to the owning agency when the imaging and extraction process is complete. The contractor shall support the tracking and monitoring of all related shipping costs identifying all costs to the DC3 Financial Manager for review.

C.4.5.5 SUBTASK 5 – DC3/CFL QUALITY ASSURANCE

The contractor shall provide assistance to DC3/CFL in maintaining, updating, and managing the Quality Assurance Program (QAP) as documented in the ASCLD/LAB ISO 17025. The contractor shall support the maintenance, updating and management of the DC3/CFL Quality Manual and the Personnel Quality Assurance Program, defining methodologies and documenting policies, procedures, and protocols within DC3 DC3/CFL.

The contractor shall maintain the DC3/CFL QAP to include performance metrics to measure the lab's effectiveness, formal and informal reviews of analyses, and methods to ensure quality and customer satisfaction.

The contractor shall support and implement goals, milestones, and objectives mandated by the ASCLD/LAB ISO 17025. The contractor shall assist the DC3 TPOC in ensuring the QAP is run in accordance with the Quality Manual to ensure accreditation of the facility by the ASCLD/LAB ISO 17025.

The contractor shall support a project plan to guide the metrics program. The project plan shall present a structured approach to maintaining and implementing the metric program. The contractor shall develop and maintain the most efficient organizational structure for implementing and managing the program. The plan shall include the overall methodology for identifying, gathering, and analyzing the measures as well as identifying participants and stakeholders, milestones/schedule, and deliverables.

The contractor shall work with each DC3/CFL Section's Chief to identify the objectives and core processes they support to ensure inter-connectivity and joint accountability of the strategy across DC3/CFL and DC3. The contractor shall assist each Section's Chief to refine their existing missions and sub-organizational models to reinforce how they would support the overall mission and vision. The contractor shall document the following outcomes:

a. Vetted strategy with vision, mission, goals, and objectives
b. Core processes and roles and responsibilities assigned to each organization's team members
c. Initial, high-level measures for assessing the organization's success

d. Organization direction and strategy
e. Prioritized list of strategic objectives
f. Documented short-term and long-term goals

The contractor shall assist the DC3 TPOC with the development and maintenance of the DC3/CFL's and/or DC3/TSD's Procedures Manuals. The contractor shall provide input, strategy, and guidance on updating, enhancing, and developing procedure manuals for DC3.

C.4.5.6 SUBTASK 6 – DC3/CFL TRAINING DEVELOPMENT AND MENTORING PROGRAM

To remain on the cutting edge of advances in D/MM forensic technology, DC3/CFL personnel require continual training. The contractor shall support DC3/CFL by monitoring, updating, and tracking all DC3/CFL personnel (contractor and Government) training through completion to maintain currency and adherence to the QAP.

The contractor shall assist the maintenance of a database containing all DC3/CFL personnel credential information to include examiners and forensic support staff working in the DC3.

The contractor shall track and monitor education and training, court appearances and testimony, examinations performed, and peer reviews performed. The contractor shall assist with the creation and population of the credentials database.

The contractor shall query credential data and create a quarterly report on certification and training status. The Credentials Management Database shall categorize and track D/MM Forensic Examiners' proficiency levels as described in the DC3/CFL Employee handbook.

The contractor shall assist DC3 with establishing and maintaining requirements for a D/MM Forensic Examiner Proficiency Testing Program.

The contractor shall incorporate test results into the Personnel Quality Assurance Program and advise the TPOC on future actions for proficiency testing.

The contractor shall assist in developing and maintaining a remedial action plan to ensure all Forensic Examiners successfully complete proficiency tests as required by the QAP to perform forensic work in DC3/CFL.

The contractor shall assist the DC3 with the establishment and management of a D/MM forensic examiner mentoring program to assist in the training of all new DC3/CFL employees in accordance with the DC3/CFL Employee handbook and DC3 SOPs. The contractor shall ensure all new employees are assigned a mentor to provide guidance through site-specific policies, initial tasks, and training. The contractor shall document the effectiveness of the mentor program and provide input on strategies to improve the new employee transition in program at DC3/CFL.

C.4.6 TASK 6 – DC3/TSD OPERATIONAL SUPPORT

The contractor shall assist the DC3/TSD with its mission to provide legally and scientifically accepted standards, techniques, methodologies, research, tools, and technologies on digital forensics and cyber threat analysis to meet current and future threats. The contractor shall assist DC3/TSD with pioneering digital forensic and cyber threat analysis tools, processes, and procedures to ensure DC3 remains on the leading edge of the discipline. The contractor shall assist DC3/TSD in managing the planning, programming, and execution of program and

infrastructure requirements linked to advancing digital forensic and cyber threat analysis research, development, test, and evaluation efforts.

Performance at off-site locations shall be determined by the DC3/TSD Director and final approval by the COR and TPOC is required.

C.4.6.1 SUBTASK 1 – DC3/TSD SYSTEMS DEVELOPMENT

The contractor shall assist with the planning, design, development, and deployment of computer forensics and cyber threat analysis capabilities efforts. The capabilities developed in support of this task consist of short to long term software development projects. Once developed, these capabilities are property of the Government.

The new development projects range from large, complex modernization efforts to a smaller file parsing effort. Historically, new development projects of large scale have required five or more resources, medium scale projects up to four resources, and smaller scale projects up to two resources. On average per year, DC3/TSD does approximately two to three large scale projects, three medium scale projects, and 11 small scale projects. There were approximately ten operations and maintenance (O&M) projects that required approximately five releases each a year.

The contractor shall support the incoming project requirements at DC3/TSD which are generated from internal DC3 customers (Directorates) as well as external customer agencies (i.e., SOCOM, NSA, NMEC, etc.). Customer project initial requirements are delivered to DC3/TSD in a formal process called a Form 10. The contractor shall assist DC3/TSD with creating, reviewing, prioritizing, and tracking requests. The contractor shall review requests for existing solutions as well as commonalities with other solutions and document those identified commonalities.

The contractor shall ensure all established requirements requests are in line with agency regulations, Federal law, the Uniform Code of Military Justice, DC3 SOPs and Quality Assurance guidelines, and the DC3 Personnel Handbook in developing computer software and performing forensic tests of computer forensic software. The contractor shall provide a written analysis of all requests that are outside the scope or problematic to such regulations.

The Government's desire is to use COTS or already existing GOTS products (hardware/software) at DC3. During the planning phase, as defined in the DC3/TSD System Development Lifecycle SOP, the contractor shall complete an alternative analysis by searching for existing COTS and GOTS solutions.

The contractor shall be responsible for creating the system concept, capturing requirements, design, development, testing, deployment, and O&M. The contractor shall, for all priority projects as defined by the Government, develop a project plan including, but not limited to, objectives, tasks, resources, milestones, and deliverables to address the requirements **(Section F, Deliverable 45).** All projects are required to be tracked in a project management tool in accordance with DC3.

The contractor shall work with all system stakeholders during requirements gathering to ensure the requirements are accurate, documented, and approved before design. The contractor shall ensure the design meets all functionality requirements, platform requirements, and security requirements prior to development and integration. The design plan shall be approved by the Government before development and integration.

The contractor shall ensure systems development efforts adhere to the applicable design specifications.

The Government currently uses a hybrid approach of Waterfall and Agile methodologies. However, the contractor may propose alternative solutions as a part of its design plan to be approved by the Government. Unless otherwise specified by the Government, the contractor shall adhere to the guidelines specified in the DC3/TSD System Development Lifecycle SOP including secure coding practices following the RMF.

The contractor shall provide testing and evaluation on deployed systems through a User Acceptance Testing (UAT) plan. The contractor's UAT results shall include, but are not limited to, discrepancies, recommendations, corrections, and document all relevant information in DC3 project documentation.

The contractor shall develop a deployment plan and prepare production environments (i.e., build, write scripts, etc.) in collaboration with ITD. The contractor shall ensure operational readiness with all appropriate stakeholders prior to deployment.

The contractor shall support O&M of deployed and operational systems. System O&M activities include, but are not limited to, bug fixes, system enhancements, preventative maintenance, and technical refresh. The contractor shall coordinate with all appropriate stakeholders when conducting O&M activities and track all requirements. All system enhancements require a formal project plan.

The contractor shall provide technical editing support for documents such as, but not limited to, validations reports, requirement and design documents, and memorandums for the record (MFRs). The technical editor shall collaborate with developers, testers, and SMEs, and ensure that each piece of content meets organizational objectives.

For specific project requirements, the contractor shall directly support operational needs in DC3/CFL, AG, and DC3/DCISE by embedding developers to work alongside forensic examiners, intrusion analysts, and cyber threat analysts. The contractor shall track such operational support activities, including the need fulfilled, time spent, and operational impact. When such operational support generates a new tool, process, or procedure that can be reused by others, the contractor shall assist with transitioning new capabilities to be a part of DC3's routine/automated processes.

The contractor shall provide an electronic WAR to include updates of status and progress of current and upcoming projects**.** The contractor shall track projects' status and identify time accrued on particular requests. The contractor shall prepare monthly briefings on the progress, outcome, or evaluation of requirements.

Dependent upon the nature of the requirement, the contractor shall gather, analyze, and prioritize existing research and informal studies to identify and collect publicly available information/tools to support and enhance DC3/TSD research and development activities leading to forensic technical solutions. Based on findings, the contractor shall provide written analysis and recommendation of further DC3/TSD research and development ideas/strategies as needed. The contractor shall document research, analysis, studies, and recommendations in written technical reports; information, point, white, and decision papers; or, MFRs.

The contractor shall participate, present, and provide input at briefings, meetings, conferences, panels, online forums, boards, seminars, working group sessions, technical exchanges, and

public for/on cyber-crime and forensic-related IT media research and development.

C.4.6.2 SUBTASK 2 – TESTING AND EVALUATION

The contractor shall assist DC3/TSD with the planning, establishment, and operations for tests, validations, and evaluations of computer, computer forensic processes, hardware and/or software in compliance with the DC3 Test and Evaluation SOPs. Validations are completed for DC3/CFL in accordance with the ASCLD/LAB. The components of which include, but are not limited to, creating test data sets, developing a test plan, carrying out the tests in a scientific manner, and generating reports outlining the test findings along with any anomalies and/or observations which could prove useful to digital forensic examiners when employing the given tool or procedure. Upon Government request, the contractor shall also prepare Project Status Review presentations which serve to document the steps undertaken by the contractor to validate that a given digital forensic tool, process, or procedure is forensically sound. The contractor should assist in automating the testing process.

Dependent upon the nature of the requirement (i.e., validation of commercial tools, testing of in-house developed software, enterprise project) the contractor shall gather, analyze, and prioritize existing data to identify and document possible testing scenarios and additional required hardware, software, or internal/external support required to complete the test in accordance with the scheduled timeframe. The contractor shall communicate, meet, and interface as a part of a team with other members assigned to a project including but not limited to developers, project managers, other testers, customers, IT support (IA).

C.4.7 TASK 7 – DC3/DCISE SUPPORT

DC3/DCISE's mission is to sustain a collaborative environment for USG and DIB entities to share actionable threat information ensuring the protection of unclassified DoD information transiting or residing on DIB information systems and networks. DIB CS Program participation was approximately 108 partners at the close FY14, 128 at the close of FY15, and 163 at the close of FY16 third quarter (Q3). Over the life of the contract, DIB CS Program participation is expected to grow over the life of the contract. The contractor will be required to adjust staff resources and operations accordingly to support the growth.

DC3/DCISE also serves as the focal point for all DIB cyber incident reporting. Supply all source derived relevant analysis including methods, indicators, and targeting objectives, while coordinating the collection and forensic analysis of submitted media/malware.

C.4.7.1 SUBTASK 1 – DEFENSE INDUSTRIAL BASE CYBERSECURITY (DIB CS) PROGRAM OFFICE AND POLICY SUPPORT

The contractor shall serve as a liaison for DC3 and provide subject matter expertise to the DoD Chief Information Officer's DIB CS Program Office to include communication on DC3 equities on DoD and national policy, to prepare DoD cyber policy recommendations, represent DC3 at DoD and interagency forums, and assist the DIB CS Program Office on a day-to-day basis. The contractor shall provide a range of subject matter expertise on DoD policy formulation, foreign cyber threats, DoD CI, the intelligence community, and DoD sensitive activities. The contractor shall interpret draft policy issuances and provide DC3 guidance on how they may impact the DC3 mission to support cyber threat information sharing, as well as its other mission areas in support of LE and CI investigative support activities, (e.g., digital forensics and multi-media

analysis for the Defense LE/CI Components, DoD cyber technical training, research, development, test, and evaluation, and cyber analytics).

The contractor shall perform outreach and represent DC3 and the DIB CS Program Office at specified Government and industry sponsored events, meetings, and conferences.

C.4.7.2 SUBTASK 2 – DIB MISSION SUPPORT

The DC3/DCISE Mission Support Division of the DIB is comprised of two branches, Customer Engagement (CE) and Organizational Readiness (OR). CE is the operational entry point for DIB Partners and USG Stakeholders. This branch is primarily responsible for all external customer support, including DIB Onboarding, DIBNet Management and outreach services to promote DIB participation, communication and collaboration in the DIB CS Program, and DIB Partner Technical Exchanges. The OR branch is primarily responsible for the internal DC3/DCISE training program, In/Out Processing of DC3/DCISE employees, managing the Metrics Database, and Logistics and DC3/DCISE knowledge management.

The contractor shall develop, manage, and coordinate DIB partner outreach projects and collaborative initiatives. Project and initiatives include, but are not limited to, outreach and communications events, campaigns, strategies, and other informational materials to promote programs. The contractor shall organize all logistics, facilities, and marketing aspects of DIB partner events (e.g., TechEx). The contractor shall serve as the primary POC for DIB partner outreach as well as requests for assistance and frequently asked questions (FAQs) from Government and industry customers. Contractor support may require the use of diverse, multi-media equipment, including audiovisual platforms, teleprompter, videotape documentation, lighting, sound reinforcement, interactive content and VTC services, and the Defense Collaboration Services platform.

The contractor shall provide graphics support for the planning and designing of concepts to represent internal and external communications initiatives. The contractor shall develop imagery, design, templates and layout for websites, email marketing blasts, newsletters, white papers, brochures, articles, and other written documents as needed to promote DIB participation.

The contractor shall develop and maintain SOPs for all program DC3/DCISE/DIB related activities**.**

The contractor shall implement and manage a formal training on DC3/DCISE processes and procedures, including technical job related functions. The contractor shall assist DC3 with the establishment and maintenance of a database containing all DC3/DCISE personnel credential information.

C.4.7.3 SUBTASK 3 – DC3/DCISE ORGANIZATIONAL QUALITY ASSURANCE AND TRAINING

The contractor shall document organizational processes and procedures performed in DC3/DCISE and maintain information on a Government-accessible channel. The contractor shall ensure DC3/DCISE processes and procedures are documented and aligned to all Capability Maturity Modeling Integration for Services (CMMI-SVC) efforts. The contractor shall lead CMMI-SVC (ML-3) re-appraisal efforts, including internal organizational coordination and collaboration, planning sessions, pre-audits, and third-party coordination evaluation.

The contractor shall provide compliance status updates to the TPOC that offer recommendations that ensure successful re-appraisal.

The contractor shall support DC3/DCISE by monitoring, updating, and tracking all DC3/DCISE personnel training through completion to maintain currency and adherence to CMMI requirements.

C.4.7.4 SUBTASK 4 – DIB PORTAL AND KNOWLEDGE MANAGEMENT SUPPORT

The contractor shall provide support for the classified and unclassified DIBNet customer portal and knowledge management in support of program operations.

The contractor shall provide DIBNet portal management (classified and unclassified) including, but not limited to, user account administration (add/delete/reset), coordination with ITD for DIBLan accounts, PKI Certification processing and tracking, troubleshooting user issues, on-boarding for new users, training, and other customer support requests as required. The contractor shall notify DC3/DCISE immediately of outages or other issues impacting the access and performance to DIBNet. The contractor shall develop metrics and track performance of DIBNet and recommend improvements to the overall DIBNet performance and process. The contractor shall provide WARs to DIB CS PMO and DC3/DCISE leadership on portal activity**.**

The contractor shall develop and implement creative and effective ways to strategically capture and share technical knowledge, recommend processes and procedures, and improve the effectiveness of DC3/DCISE and DIB CS programs. The contractor shall monitor and maintain program content, including the development of ad-hoc reports, queries, and analyses. The contractor shall support customer requests (i.e., Requests for Information (RFIs)) and collection management from internal and external mission partners. The contractor shall identify process improvements and develop a performance measurement framework for programs. The contractor shall maintain quality control of products residing on the systems. The contractor shall develop and maintain SOPs**.**

C.4.7.5 SUBTASK 5 – DC3/DCISE CYBER THREAT ANALYSIS SUPPORT

The contractor shall provide cyber threat analysis support for the DC3/DCISE Analytics Division on behalf of the DIB community. The contractor shall provide an interface with the DIB-CERT to receive and provide initial response to cyber security events reported by DIB partners (historical workload metrics provided below). The contractor shall provide support to analyze partner triage reporting and ensure that threat, vulnerability, and mitigation information is disseminated in a timely and effective manner. This include identifying indicators of compromise (IOCs), conducting methods of entrenchment, mining file systems, and identifying network threats, vulnerabilities, and exploits. The contractor shall conduct a variety of cyber intelligence gathering methods, including Open Source Intelligence (OSINT) and closed source intelligence gathering, source verification, data fusion, and link analysis. The contractor shall also conduct malware analysis on specific cases. The contractor shall develop analytical report products derived from analysis to assist partners with implementing defensive measures.

Additionally, the contractor shall:

a. Perform acceptance of the initial reporting of cyber security events from DIB partners in accordance with the defined timeline and DC3/DCISE SOP.

b. Produce initial report on severity of reported cyber security event in accordance with the defined timeline and DC3/DCISE SOP.
c. Perform data mining in support of customer requirements, to include basic tool development, database development, and other tasks as defined by best practice software development lifecycle management.
d. Plan, coordinate, and execute off-site quarterly technical exchanges with external entities.
e. Coordinate receipt of copies of malware (receiving copies of the actual offending software code and medium by which it was transmitted, which created the computer security event or incident), logs, and affected media.
f. Develop and deliver Customer Response Forms (CRF) after receipt of Incident Collection Form (ICF).
g. Develop and deliver Technical Analysis Reports (TAR) after ICF receipt.
h. Develop and deliver Cyber Targeting Analysis Reports (CTAR).
i. Develop and deliver the daily Threat Information Product (TIP) Report notifying DIB Partners of possible threats to their network infrastructure, based on indicators derived solely from reports on intrusion activity in USG Stakeholder networks.
j. Develop and deliver CRF Supplements (amplifying information) to DIB Partners.
k. Develop and deliver DIB Alerts within four hours of a reported incident or security event to help DIB Partners identify potential compromised systems within their networks.
l. Develop and deliver Damage Assessment Management Office (DAMO) reports for further evaluation.
m. Support development and delivery of annual updates to the DC3/DCISE Long Range Strategic Plan.
n. Provide regular updates regarding threats and trends via report tracker and meetings.

DC3/DCISE currently supports 168 members in the DIB partner community. In FY15, the activity from the DIB partner community included 636 voluntary and 23 mandatory submission requirements. The DC3/DCISE Analytics Division produced 422 CRFs, 79 Supplements, 16 CTARs, 16 DAMOs, 10 DIB Alerts, 26 TARs, and 165 TIPs.

The contractor shall provide Quality Control (QC) support in the process of evaluating techniques, methods, and activities to consistently maintain product report quality standards. The QC support implements and manages the QC process used by DC3/DCISE prior to and after releasing all deliverables to internal and external stakeholders. The contractor shall provide the Government TPOC with final products for peer review before delivery. The goal of QC is to provide the best quality product with minimal disruption to the workflow process. QC reviews other DC3/DCISE publications and correspondence as well, including SOPs, training presentations, letters, briefing slides, conference brochures and papers, and other communications.

C.4.8 TASK 8 –DC3-AG OPERATIONS SUPPORT

The contractor shall provide operations and technical support for the DC3-AG mission. The contractor shall provide a project management solution, inclusive of collecting and analyzing program and ad-hoc project metrics, resource management, quality assurance, and developing and implementing program improvements. The contractor shall support the development and

execution of the AG analyst training program. The contractor shall identify technologies to increase the efficiency and effectiveness of analysis services and test technologies and create system/software development requirements for the DC3/TSD as required.

The contractor shall maintain DC3-AG related information on websites and via internal knowledge management sources across multiple classified environments and make recommendations to improve the overall operational effectiveness of these systems. The contractor shall develop and deliver a WAR to the DC3-AG Director which provides updates on the entire staff's activities during the preceding week and illustrates the current product production levels**.**

The contractor shall conduct cyber intelligence analysis to develop DC3-AG products and services. These high value cyber analysis/linguist products and services support LE/CI agencies in critical investigations and operations; principal among these agencies are AFOSI, NCIS, and FBI. The contractor is responsible for maintaining a strict quality assurance process that inspects all products for analytic and technical accuracy. The contractor shall provide the Government TPOC with final products for peer review before delivery.

The contractor shall conduct all source cyber analytical/linguist fusion for cyber investigations/ops. The contractor shall support analysis and cuing for CI operations in cyberspace against Advanced Persistent Threats (APTs). The contractor shall provide a complete picture of the Tactic, Techniques, and procedures (TTPs) used by the attacker through fusion analysis of the media, information provided LE/CI community. Though "actionable intelligence" will be identified primarily for LE/CI organizations, the information may also be tailored to multiple disciplines, to include computer network defenders, signals intelligence (SIGINT) and human intelligence (HUMINT) operators, intelligence analysts, and policy/decision makers. In addition, but not limited to, the contractor shall provide the following Products and Services:

a. Develop and deliver Tailored Operating Picture (TOP) products that evaluate advanced persistent threat TTP activities, attribute those activities and track the activity over time on a regularly schedule timeline defined by the AG Director determined by activity level.
b. Develop and deliver Weekly Assessment of intrusion activity that includes a short list of the associated new reporting, "so what" of recent reporting.
c. Develop and deliver Weekly Operational Lead Reports that attribute technical intrusion data to the requesting organization. These reports are used as leads for investigative and operational purposes.
d. Develop and deliver Profile products on APT actors, organizations and relationships for investigative lead purposes.
e. Develop and deliver Cyber Intelligence Analytic products on emerging topics, and on the tactics, techniques and procedures, and attribution characteristics of APTs.
f. Develop and deliver Intelligence Information Reports (IIRs) for distribution within the IC.

The contractor shall provide technical editing support for all IIRs products. The IIRs shall maintain accuracy and standardization of format and style to AF and LE/IC requirements. The contractor shall collaborate with writers and SMEs, and ensure that each piece of content meets organizational objectives. The contractor shall appropriately store and update products as

necessary with guidance from office leadership.

The contractor shall lead a collaborative analytical and technical exchange with SMEs from LE/CI, CND, IC, and IA agencies. Long distance travel (CONUS and OCONUS) is anticipated to be required in support of these efforts. The objective of this exchange is to build a threat picture to enable proactive LE/CI cyber operations focused on nation-state threat actors. In support of these efforts, the contractor shall:

a. Develop analyst engagement opportunities, manage liaison functions, and deliver analyst notes of the minutes of each meeting.
b. Develop and deliver a Quarterly Meeting featuring quarterly updates of APT activities and topics of interest by region and current topics being discussed among interagency analyst working groups.
c. Develop and deliver daily DNS Tool updates to DC3-AG's mission partners.
d. Provide process and capabilities to manage RFI processing.
e. Create mission engagement materials as necessary.

The contractor shall coordinate all incoming and processing of media and malware cases submitted by DC3-AG partner agencies for analysis. The contractor shall manage the workflow of all malware and systems submissions cases coming to DC3-AG for analysis and generates workflow statistics. The contractor shall provide a weekly update brief to the DC3-AG leadership on the workflow.

C.4.9 **TASK 9 – DEFENSE VULNERABILITY DISCLOSURE PROGRAM (DVDP) OPERATIONAL SUPPORT**

The contractor shall assist the DC3 with its mission to improve defense of the DoD Information Network (DoDIN), by managing capabilities to receive, validate, and disseminate cybersecurity vulnerabilities reported by private-sector researchers. The contractor will also assist DC3 to track and analyze reported vulnerabilities and mitigation actions by system owners to identify gaps in DoDIN defenses; areas requiring increased attention, and areas for improvement.

C.4.9.1.SUBTASK 1 – RECEIVE, VALIDATE, AND PROCESS NEW DVDP REPORTS [Report Mgt Team]

The contractor will receive, validate, and process vulnerability reports from private-sector researchers submitted under the DVDP. The contractor will review all DVDP reports to determine if they are within the scope of the DVDP policy and will compare new DVDP reports with previously submitted DVDP reports to identify duplicates. The contractor will close all DVDP reports determined to be duplicates or out-of-scope. The contractor will also close any DVDP reports where the reported vulnerability has been determined by the system owner to be an accepted risk, or where the vulnerability is pending mitigation per an approved Plan of Action and Milestones (POAM). The contractor will recommend closing appropriate DVDP reports as informative, but not requiring further action and will recommend referral of DVDP reports to other government agencies as appropriate. If new DVDP reports do not provide sufficient detail

for the contractor to make these assessments, the contractor will identify the deficiency and communicate this information to the reporting researcher.

C.4.9.2 SUBTASK 2 – VALIDATE REPORTED VULNERABILITIES [Vulnerability Validation Team]

The contractor will assess vulnerabilities reported under the DVDP to validate the information provided by the private-sector researchers. The contractor assessment will include replicating the actions taken by the researchers to identify the reported vulnerability. If additional information is required to validate the reported vulnerability, the contractor will determine and document the additional information needed from the researcher in order to conduct this assessment. The contractor will identify DVDP reports with confirmed vulnerabilities for mitigation action by the affected DoD component. The contractor will identify DVDP reports with vulnerabilities that cannot be validated and will provide recommendations for disposition of theses DVDP reports.

C.4.9.3 SUBTASK 3 – IDENTIFY SYSTEM OWNERS [Report Mgt Team – USCC Funded]

The contractor will review the DoD DMZ Whitelist to determine the owners of systems with vulnerabilities identified by DVDP reporting. For systems identified in the DMZ Whitelist, the contractor will document all detailed organizational/individual contact information so that it can be provided to JFHQ-DoDIN in order to facilitate tasking to the appropriate DoD Component. For systems that cannot be identified in the DMZ Whitelist, the contractor will use available information to identify and contact system owners. The contractor will obtain and document all detailed organizational/individual contact information required for the DMZ Whitelist so that it can be provided to JFHQ-DoDIN in order to facilitate tasking to the appropriate DoD Component. This information will also be provided to the Defense Information Systems Agency (DISA) so that they may update the DMZ whitelist. The contractor will establish and maintain a separate list of all DoD managed websites and web applications that are not on the DoDIN.

C.4.9.4SUBTASK 4 –IDENTIFY RELEVANT VULNERABILITY GOVERNANCE [Vulnerability Validation Team – USCC Funded]

The contractor will review validated DVDP reports to identify existing DoD cybersecurity governance relevant to the reported vulnerability. The contractor will identify specific Security Technical Implementation Guide (STIG) and/or Risk Management Framework (RMF) security controls that may be relevant to the reported vulnerability. This information will be documented so that it can be provided to JFHQ-DoDIN to facilitate mitigation actions by the affected Component.

C.4.9.5SUBTASK 5 – TRANSMIT VALIDATED DVDP REPORTS TO JFHQ-DoDIN [Report Mgt Team]

The contractor will forward validated DVDP reports with validated vulnerabilities to JFHQ-DoDIN in order to facilitate tasking to the appropriate DoD Component. The contractor will integrate the initial DVDP report from the researcher; report and vulnerability validation results; system owner contact information; and relevant governance documentation for transmittal to JFHQ-DoDIN via the DoD Secret Internet Protocol Router network (SIPRNet). The contractor will confirm receipt of the DVDP report package by JFHQ-DoDIN.

C.4.9.6SUBTASK 6 – COORDINATE OPEN DVDP REPORTS WITH PRIVATE-SECTOR RESEARCHERS AND DOD COMPONENTS
[Report Mgt Team]

The contractor will maintain appropriate communication with private-sector researchers, JFHQ-DoDIN, and DoD Components on all open reports. The contractor will ensure inquires, updates, and other communications are promptly and properly coordinated with all appropriate parties to maintain shared situational awareness on the processing and status of DVDP reports.

C.4.9.7SUBTASK 7 – VALIDATE REPORTED MITIGATION ACTIONS [Vulnerability Validation Team]

The contractor will assess actions taken by DoD Components in order to validate that vulnerabilities reported by private-sector researchers under the DVDP are effectively mitigated. The contractor assessment will include replicating the actions taken by the researchers to determine if the reported vulnerability has been mitigated. The contractor will recommend closure of DVDP reports with mitigated vulnerabilities and will recommend returning reports with unmitigated vulnerabilities to JFHQ-DoDIN for further action.

C.4.9.8SUBTASK 8 – RETURN REPORTS WITH UNMITIGATED VULNERABILITIES TO JFHQ-DODIN [Report Mgt Team]

The contractor will return DVDP reports with unmitigated vulnerabilities to JFHQ-DoDIN via SIPRNET in order to facilitate re-tasking to the appropriate DoD Component. The contractor will include the steps and results of the assessment conducted which determined the vulnerability was still present. The contractor will confirm receipt of the returned DVDP report package by JFHQ-DoDIN.

C.4.9.9SUBTASK 9 – CLOSE REPORTS WITH MITIGATED, POAM'D, OR ACCEPTED VULNERABILITIES [Report Mgt Team]

The contractor will close DVDP reports with mitigated vulnerabilities and notify the researcher. The contractor will also close DVDP reports and notify the researcher if the system owner has accepted the risk of an unmitigated vulnerability or has an approved POAM to mitigate the vulnerability at a later date.

C.4.9.10 SUBTASK 10 –AFTER ACTION ASSESSMENT [Report Mgt Team]

The contractor will develop an after action assessment to be completed by owners of DoD systems with validated vulnerabilities. The contractor will collect, aggregate, and analyze the information provided by the system owners to identify gaps in DoDIN defenses; areas requiring increased attention, and areas for improvement. The contractor will publish a quarterly report documenting the results of these assessments and include recommendations to improve DoDIN defenses.

C.4.9.11 SUBTASK 11 – FOLLOW-UP ON MISSING AND INCOMPLETE AFTER ACTION ASSESSMENTS [Report Mgt Team]

The contractor will follow-up on missing and incomplete after action assessments through JFHQ-DoDIN via SIPRNET in order to obtain the after actin assessment from the appropriate DoD Component. The contractor will confirm receipt of the completed after action assessment from JFHQ-DoDIN.

C.4.9.12 SUBTASK 12 – REVIEW AND AUTHORIZE PUBLICATION OF VULNERABILITY REPORT FINDINGS [Report Mgt Team & BTO/PAO Team]

The contractor will notify DC3 Public Affairs (PA) personnel if a researcher requests public disclosure of their report and draft a summary of the DVDP report for public release. DC3/PA will review the proposed public release to ensure compliance with OSD/PA policy governing the publication of DVDP reports. Upon approval by DC3/PA, the contractor will provide the researcher with the report summary approved for public release.

C.4.9.13 SUBTASK 13 – LE/CI/IC DECONFLICTION OF DVDP REPORTING [Report Mgt Team & AG]

The contractor will deconflict DVDP reporting with LE/CI/IC reporting. The contractor will monitor LE/CI/IC reporting concerning adversary targeting of DoD networks and systems. The contractor will correlate relevant LE/CI/IC reporting with DVDP reporting. Any identified correlations of DVDP and LE/CI/IC reporting will be documented and reported to the government lead for action. The contractor will receive requests for information (RFI) from LE/CI/IC personnel regarding specific DVDP reports and researchers. The contractor will prepare appropriate responses for approval by the government lead.

C.4.9.14 SUBTASK 14 – COLLECT AND REPORT PROGRAM METRICS [Report Mgt Team]

The contractor will capture, aggregate, analyze, and report program process and performance measures as directed by the DoD CIO. Data to be collected, analyzed, and reported includes but is not limited to the following proposed metrics:

Vulnerability Lifecycle/Process Metrics

- Median Triage time
- Median remediation time

- Median Component remediation time by component
- Median Component remediation time per month
- Median Component remediation time by type of vulnerability
- Median Component remediation time by severity of vulnerability

Security Controls Metrics

- To identify compliance issues:
  - Percent of vulnerabilities covered by existing STIGs, IAVA/Bs, Orders, or CVEs
  - Number Vulnerabilities per existing STIG, IAVA/B, Order, or CVE: JFHQ-DoDIN
- To identify trends and drive future orders:
  - Types of root-causes reported by components
  - Percent of Vulnerabilities not covered by existing controls
  - Vulnerabilities not covered by existing controls (broken out by reported root-cause)

Vulnerability Statistics

- Total Number of Reports
  - Broken out per month by Total, Open, Closed, Resolved, Duplicate
  - Broken out by Component
- Types of validated vulnerabilities
  - Number per month
- Severity of validated vulnerabilities
  - Number per month
  - median severity over time

The contractor will capture, aggregate, analyze, and report Task Order performance measures as specified in the Quality Control Plan for this Task Order

C.4.9.15 SUBTASK 15 – MAINTAIN DVDP REPORT MANAGEMENT SYSTEM [DC3/TSD & BTO/ITD]

The contractor will maintain the DVDP Report Management System to sustain capabilities delivered by the successful execution of SUBTASK 16. This includes, but is not limited to, software and hardware fixes and any necessary upgrades. Major upgrades to the system that deliver new capabilities will be managed as separate subtasks.

C.4.9.16 SUBTASK 16 – DESIGN, DEVELOP, & IMPLEMENT DVDP REPORT MANAGEMENT SYSTEM [DC3/TSD & BTO/ITD – Base Year Only]

The contractor will design, develop, accredit, and implement a DVDP Report Management System. High-level requirements for this system include, but are not limited to:

- Export of new and changed data from the HackerOne system and import to the system on SIPRNET
- Identification and documentation of system owners

- Identification and documentation of relevant IAVMs, STIGS, and RMF controls
- Dissemination of DVDP reports and attachments to JFHQ-DoDIN, the Components, and system owners
- Tracking the status of DVDP reports as they are processed, disseminated, and resolved
- Capture and reporting of After Action Assessment data
- Capture and reporting of Metrics data for DoD CIO

C.4.9.17 SUBTASK 17 – DVDP IT INFRASTRUCTURE BUILD-OUT [BTO/ITD – Base Year Only]

The contractor will design, develop, accredit, and implement the IT infrastructure necessary to support the DVDP staff and operations. High-level requirements for this infrastructure include, but are not limited to:

- DEN, SDEN, and ONET systems for all workstations/staff
- Network Printers, scanners, and digital senders on DEN, SDEN, and ONET
- Desk phones for all workstations/staff
- Secure phone for Director
- DEN and SDEN VTC capability
- Conference call capability
- DEN, SDEN, and ONET video projection capability

C.4.10 TASK 10 -TRANSITION-IN

The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. All transition activities shall be completed 45 calendar days after TO start date. The updated Draft Transition-In plan shall be presented at the kick-off meeting **(Section F, Deliverable 03)** and submitted for final approval within three days following the kick-off meeting **(Section F, Deliverable 04).**

C.4.10.1 SUBTASK 1 – IMPLEMENT TRANSITION-IN PLAN

The contractor shall begin implementing its Transition-In Plan no later than (NLT) ten calendar days after award or upon Government approval of the draft Transition-In Plan.

C.4.11 TASK 11 -TRANSITION-OUT

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a Transition-Out Plan NLT 90 calendar days prior to expiration of the TO **(Section F, Deliverable 61).** The contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes
b. Points of contact

c. Location of technical and project management documentation
d. Status of ongoing technical initiatives
e. Appropriate contractor to contractor coordination to ensure a seamless transition
f. Transition of Key Personnel
g. Schedules and milestones
h. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

C.4.11.1 SUBTASK 1 – IMPLEMENT TRANSITION-OUT PLAN

The contractor shall begin implementing its Transition-Out Plan no later than (NLT) 90 calendar days prior to expiration of the TO.

C.4.12 TASK 12 – DC3 SURGE SUPPORT

DC3's mission is subject to constant technological and operational change. As such, the contractor shall support the objective of keeping DC3's technological and mission capabilities congruent with developments and changes in the fields of D/MM forensics, cyber security, and IT through a surge capability.

The surge capability shall provide staff resources for unplanned projects or unexpected events (on-call 24x7 support) in the task areas identified throughout the TO. For example: time-sensitive lab case, DIB security-sensitive request, new technology implementation, system modernization, building renovation or relocation, forensic lab upgrades, policy impacts, and national security/critical events. Project based surge efforts are anticipated to last six months to a year.

In support of project based surge efforts, the contractor shall develop a comprehensive project plan, inclusive of project scope, requirements, milestones, deliverables, and resource/cost information **(Section F, Deliverable 62)** to be approved by the Government prior to project start. The contractor shall staff Surge resources within 30 days of formal written approval of the Surge Support Plan.

This page intentionally left blank.

E.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports, and other deliverables under this TO will be performed by the FEDSIM Contracting Officer's Representative (COR) with participation from all DC3 Technical Points of Contact (TPOC) at the designated performance locations.

E.2 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the FEDSIM COR. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

E.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be in compliance with the requirements set forth in the TO, the contractor's proposal, and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

For IT development, the final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables shall either be incorporated in the succeeding version of the deliverable, or the contractor shall explain to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the quality assurance requirements stated within this TO, the document may be rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the FEDSIM COR.

E.4 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in Section F) from Government receipt of the draft deliverable. Upon receipt of the Government comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

E.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The FEDSIM CO/COR will provide written notification of acceptance or rejection **(Section J, Attachment R)** of all final deliverables within 15 workdays unless specified otherwise in Section F). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.6 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies shall be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor shall immediately notify the FEDSIM COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

If the contractor does not provide products or services that conform to the requirements of this TO, the Government will document the issues associated with the non-conforming products or services in the award fee determination report, and there will be an associated reduction in the award fee earned.

F.1 PERIOD OF PERFORMANCE

The period of performance for this TO is a one-year base period and four, one-year options.

Base Period:	January 19, 2017 to January 18, 2018
Option Period 1:	January 19, 2018 to January 18, 2019
Option Period 2:	January 19, 2019 to January 18, 2020
Option Period 3:	January 19, 2020 to January 18, 2021
Option Period 4:	January 19, 2021 to January 18, 2022

F.2 PLACE OF PERFORMANCE

The primary place of performance is onsite at DC3's facilities in Linthicum, MD. The secondary sites include NMEC in Northern Virginia, the NCIJTF in Chantilly, VA and the DIB in Alexandria, VA.

Long distance travel is required (CONUS and OCONUS) to provide support for DC3 mission activity, including evidence examination, litigation, training, conferences/seminars/workshops, technical briefing to customer or other DoD entity, testimony in military courts martial or other state, Federal, local, or tribal court associated to digital forensic exam conducted by examiner.

F.3 TO SCHEDULE AND MILESTONE DATES

The following schedule of milestones will be used by the FEDSIM COR to monitor timely progress under this TO.

The following abbreviations are used in this schedule:

N/A: Not Applicable

NLT: No Later Than

All references to days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend. The contractor shall deliver the deliverables listed in the following table:

DEL. #	DIR.	MILESTONE/ DELIVERABL	TO REF.	PLANNED COMPLETION DATE	DATA RIGHTS
01	N/A	Kick-Off Meeting		Within 25 workdays of PS	
02	N/A	Copy of TO (initial award and all modifications)	F.4	Within 10 workdays of award	

DEL. #	DIR.	MILESTONE/ DELIVERABL	TO REF.	PLANNED COMPLETION DATE	DATA RIGHTS
03	N/A	Draft Transition-In Plan – Updated	C.4.2.1; C.4.10	Due at Kick-Off Meeting	252.227-7013
04	N/A	Transition-In Plan – Final	C.4.10	10 workdays after receipt of Government comments	252.227-7013
05	N/A	Project Management Plan – Draft	C.4.2.4	Due 10 workdays after Kick-Off Meeting and then yearly	252.227-7013
06	N/A	Project Management Plan	C.4.2.4	10 workdays after receipt of Government comments	252.227-7013
08	N/A	QCP – Updated	C.4.2.6	Due at Kick-Off Meeting, updated annually or upon request.	252.227-7013
09	N/A	Monthly Status Report	C.4.2.6	As required	252.227-7013
10	N/A	Administrative Support SOPs	C.4.3.1	As required and then yearly update	252.227-7013
16	BTO	DC3 IM SOP	C.4.3.2	As required and then yearly update	252.227-7013
22	BTO	Training Management SOP	C.4.3.8	As required and then yearly	252.227-7013
26	BTO/ITD	Network Enterprise Architecture	C.4.4.3	As required	252.227-7013

DEL. #	DIR.	MILESTONE/ DELIVERABL	TO REF.	PLANNED COMPLETION DATE	DATA RIGHTS
32	BTO	DC3 IC Design and Specs	C.4.4.6	IAW PMP	252.227-7013
33	BTO	DC3 IC IOC	C.4.4.6	Within six (6) months of formal approval of Deliverable 32 (Design and Specs)	252.227-7013
34	BTO	DC3 IC FOC	C.4.4.6	Within one (1) year of formal approval of Deliverable 32 (Design and Specs)	252.227-7013
45	DC3/TSD	Dev Project Plan	C.4.6.1	As required / IAW PMP	252.227-7013
61	N/A	Transition-out	C.4.10	NLT 90 calendar days prior to expiration of the TO	252.227-7013
62	All Applicable	Surge Support Plan	C.4.11	Within ten working days of written Government notification to proceed with Surge plan.	252.227-7013
63	All Applicable	SLA – Draft	N/A	Contractor determined	252.227-7013

DEL. #	DIR.	MILESTONE/ DELIVERABL	TO REF.	PLANNED COMPLETION DATE	DATA RIGHTS
64	All Applicable	SLA – Final	N/A	10 workdays after receipt of Governme nt comments	252.227-7013
66	N/A	TSM Meeting Minutes	C.4.2.3	Within five workdays of the meeting	252.227-7013

The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this TO. The Government reserves the right to treat non-confirming markings in accordance with DFAR 252.227-7013 and 252.227-7014.

F.4 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten workdays from the date of the CO's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a portable document format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA **(Section F, Deliverable 02).** The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall explain why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider all of the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.5 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by email and removable electronic media, as well as placing in the DC3's designated repository. The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the

market.

a. Text	MS Word
b. Spreadsheets	MS Excel
c. Briefings	MS PowerPoint
d. Drawings	MS Visio
e. Schedules	MS Project

F.6 PLACE(S) OF DELIVERY

F.7

Copies of all deliverables shall be delivered to the FEDSIM COR and DC3 TPOC at the following addresses:

Contracting Officer's Representative

Bonnie Heider
GSA FAS AAS FEDSIM
1800 F Street, NW (QF0B)
Washington, D.C. 20405
(b) (6) (mobile)
Bonnie.Heider@gsa.gov

Technical Point of Contact:

Matthew Rout, PMO
DoD Cyber Crime Center
911 Elkridge Landing Rd
Linthicum MD 21090
410-981-0050
(b) (6)

F.8 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the FEDSIM COR via a Problem Notification Report (PNR) **(Section J, Attachment Q)** as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

G.1 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The FEDSIM Contracting Officer (CO) appointed a COR in writing through a COR Appointment Letter **(Section J, Attachment A).** The COR will receive, for the Government, all work called for by the TO and will represent the CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to contractor personnel.

The COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by the CO by properly executed modifications to the Contract or the TO.

G.1.1 CONTRACT ADMINISTRATION

Contracting Officer (CO):

Andrew R. Hotaling
GSA FAS AAS FEDSIM
1800 F Street, NW, 6000 (QF0B)
Washington, D.C. 20405
Telephone: (202) 213-8818
andrew.hotaling@gsa.gov

Contracting Officer's Representative (COR):

Bonnie Heider
GSA FAS AAS FEDSIM (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: (202) 676-7136 (mobile)
bonnie.heider@gsa.gov

Technical Point of Contact (TPOC):

Matthew Rout, PMO
DoD Cyber Crime Center
911 Elkridge Landing Rd
Linthicum MD 21090
410-981-0050
(b) (6)

G.2 INVOICE SUBMISSION

The contractor shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice:

TO Number: *(from GSA Form 300, Block 2)*

Paying Number: *(ACT/DAC NO.) (From GSA Form 300, Block 4)*
FEDSIM Project Number: *DE00789*
Project Title: *DC3 Mission Support*

The contractor shall certify with a signed and dated statement that the invoice is correct and proper for payment.

The contractor shall provide invoice backup data in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category.

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Assisted Services Shared Information System (ASSIST) to submit invoices. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

https://portal.fas.gsa.gov

Log in using your assigned ID and password, navigate to the order against which you want to invoice, click the Invoices and Acceptance Reports link in the left navigator, and then click the *Create New Invoice* button. The AASBS Help Desk should be contacted for support at 877-472-4877 (toll free) or by email at AASBS.helpdesk@gsa.gov. By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. However, the FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment.

G.3 INVOICE REQUIREMENTS

The contractor shall submit a draft copy of an invoice to the client POC for review prior to its submission to GSA. The draft invoice shall not be construed as a proper invoice in accordance with FAR 32.9 and GSAM 532.9. The contractor shall submit simultaneous copies of the invoice to both GSA and the client POC. Receipts are provided on an as requested basis.

If the TO has different contract types, each should be addressed separately in the invoice submission.

The final invoice is desired to be submitted within six months of project completion.

G.3.1 COST-PLUS-AWARD-FEE (CPAF) CLINs (for LABOR)

The contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B) and by WBS element and shall be provided for the current billing month and in total from project inception to date. In addition, on a separate tab all hours shall be provided by CLIN, WBS element and by employee name. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. Employee name (current and past employees)
b. Employee company
c. Employee *Alliant* labor category

d. Exempt or non-exempt
e. Monthly and total cumulative hours worked
f. Corresponding CLIN and WBS Element where hours were billed
g. Corresponding DC3 Responsible Directorate where support was provided
h. Corresponding Alliant ceiling rate (if applicable)
i. Effective hourly rate by WBS element
j. Any cost incurred not billed
k. Labor adjustments (from any previous months (e.g., timesheet corrections))
l. Current approved forward pricing rate agreement in support of indirect costs billed

All cost presentations provided by the contractor shall also include Overhead charges and General and Administrative charges at a minimum at the cost center level and shall also include the Overhead and General and Administrative rates being applied.

The contractor may invoice after accepting the modification which includes the award fee determination and any corresponding de-obligation of unearned fee. See the Award Fee Determination Plan in **Section J, Attachment I** for additional information on the award fee determination process.

G.3.2 TOOLS AND OTHER DIRECT COSTS (ODCs)

The contractor may invoice monthly on the basis of cost incurred for the Tools and ODC CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

a. Tools and/or ODCs purchased
b. Consent to Purchase number or identifier
c. Date accepted by the Government
d. Associated CLIN
e. Project-to-date totals by CLIN and WBS Element
f. Cost incurred not billed
g. Remaining balance of the CLIN

All cost presentations provided by the contractor shall also include Overhead charges, General and Administrative charges and Fee in accordance with the contractor's Defense Contract Audit Agency (DCAA) cost disclosure statement.

G.3.3 TRAVEL

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Federal Travel Regulations (FTR) - prescribed by the GSA, for travel in the contiguous U.S.
b. Joint Travel Regulations (JTR), Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and

outlying areas of the U.S.

c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the JTR/FTR/DSSR. The invoice shall include the period of performance covered by the invoice, the CLIN number and title. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN. The current invoice period's travel details shall include separate columns and totals and include the following:

a. Travel Authorization Request number or identifier, approver name, and approval date
b. Current invoice period
c. Names of persons traveling
d. Number of travel days
e. Dates of travel
f. Number of days per diem charged
g. Per diem rate used
h. Total per diem charged
i. Transportation costs
j. Total charges
k. Explanation of variances exceeding 10 percent of the approved versus actual costs
l. Indirect handling rate
m. DC3 Directorate Traveled was required under
n. For transportation travel, POV should be broken out into its own column from transportation costs because POV reimbursement is a specific number that changes each year
o. The travel back up should be broken out the same way the TAR has the costs broken out. (For example, instead of a column stating Per Diem Used, there should be a separate column for Lodging and a separate column for M&IE).

All cost presentations provided by the contractor shall also include Overhead charges and General and Administrative charges in accordance with the contractor's DCAA cost disclosure statement.

H.1 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key." The contractor shall propose appropriate labor categories for these positions. The Government does not intend to dictate the composition of the ideal team to perform this TO. Therefore, the Government encourages and will evaluate additional Key Personnel as proposed by the offeror.

a. Program Manager
b. DC3/CFL Lead D/MM Forensic Technician Task Lead
c. DC3/CFL Lead D/MM Forensic Examiner Task Lead
d. ITD Technical Task Lead
e. DC3/TSD Technical Task Lead
f. DC3-AG Technical Task Lead
g. DC3/DCISE Technical Task Lead

The Government desires that Key Personnel be assigned for the duration of the TO.

H.1.1 PROGRAM MANAGER

It is required that the Program Manager (PM) possesses the following qualifications:

a. Project Management Professional ® Certification
b. Demonstrated experience managing a complex project, TO, or program of similar size (managing 50 or more personnel) referenced under this TO.
c. Demonstrated experience overseeing and determining manpower requirements for projects similar in scope and complexity referenced in the TO, and consisting of a diversity of technical skill sets and labor categories.
d. Demonstrated knowledge of financial and performance monitoring of contracts (e.g. performance metrics).
e. Demonstrated knowledge of DoD IT and IA standards, processes, policy, and regulations.

It is desired that the Program Manager (PM) possess the following qualifications:

a. Demonstrated experience evaluating a complex project, TO, or program to identify and eliminate operational inefficiencies.
b. Demonstrated knowledge of CS requirements similar to those referenced throughout the TOR.

H.1.2 DC3/CFL LEAD D/MM FORENSIC TECHNICIAN TASK LEAD

It is required that the DC3/CFL Lead D/MM Forensic Technician possesses the following qualifications:

a. Demonstrated experience leading technical efforts and supervising teams in a forensics lab environment similar to the scope and complexity of DC3 DC3/CFL.
b. Demonstrated experience handling digital media evidence and performing forensically sound duplication of original evidence.
c. Demonstrated knowledge of Microsoft windows, Apple/UNIX and Linux operating systems as it relates to forensics examinations.

d. Demonstrated experience utilizing various imaging tools, including those referenced in the DC3 (e.g. FTK, EnCase, Deepspar Disk Imager, and Atola).
e. Demonstrated experience conducting physical hard drive repairs, such as, head stack replacement, firmware manipulation, and circuit board work.
f. Demonstrated experience with encryption as it relates to forensic extraction examination and analysis of digital media.

It is desired that the DC3/CFL Lead D/MM Forensic Technician possess the following qualifications:

a. Demonstrated experience performing extraction and recovery techniques, such as, Hard Drive Data Recovery, Solid State Data Recovery, Chip-Off, JTAG, Encryption Bypass, Component replacement and/or repair, and 2D/3D projection imaging (X-ray machine operations).
b. Demonstrated experience extracting data from unique and complex digital media (e.g. hard drives, thumb drives, memory cards, mobile devices, gaming consoles/systems, vehicle infotainment, etc.) with a variety of interfaces such as PATA, SATA, PCIe, SAS and SCSI.
c. Demonstrated experience with soldering techniques (e.g. through-hole and surface mount technologies).

H.1.3 DC3/CFL LEAD D/MM FORENSIC EXAMINER TASK LEAD

It is required that the DC3/CFL Lead D/MM Forensic Examiner possesses the following qualifications:

a. Demonstrated experience leading technical efforts and supervising teams in a forensics lab environment similar to the scope and complexity of DC3 DC3/CFL.
b. Demonstrated experience performing D/MM forensics examinations, analysis, and techniques for LE and CI investigations.
c. Demonstrated knowledge of Microsoft windows, Apple/UNIX and Linux operating systems as it relates to forensics examinations.
d. Demonstrated experience utilizing examination tools, including those referenced in the DC3 (e.g. FTK, EnCase, and X-Ways).
e. Demonstrated knowledge of handling digital media evidence and an applied understanding of forensic technician functions.

It is desired that the DC3/CFL Lead D/MM Forensic Examiner possess the following qualifications:

a. Demonstrated knowledge of forensic examinations to support litigation cases (e.g. chain of custody, discovery requests, and expert witness testimony)
b. Demonstrated experience in malware analysis, reverse engineering, software development, and the cyber-attack lifecycle, from the initial exploit and malware execution path to callback destinations and follow-on binary download attempts.

H.1.4 ITD SERVICES TASK LEAD

It is required that the ITD Services Lead possesses the following qualifications:

a. Demonstrated experience leading and supervising teams in a networking and infrastructure environment (classified and unclassified) similar to the size, scope, and complexity or DC3.
b. Demonstrated knowledge of systems administration and systems engineering tasks, including configuring and troubleshooting desktop systems, virtualized servers, storage arrays, and network systems.
c. Demonstrated experience with the design, installation, administration and troubleshooting of desktop and networking infrastructure in a Linux, UNIX, and Microsoft operating environment.
d. Demonstrated experience with the administration, configuration and troubleshooting of LAN/WAN networks, including wireless components, firewalls, routing and switching, IPV6 and VPN.
e. Demonstrated experience with unified communications, including the design, installation, maintenance, and administration of video teleconferencing (VTC) system for multi-level classification environments (Unclassified, Secret and TS/SCI).

It is desired that the ITD Services Task Lead possess the following qualifications:

a. DoD 8570 Baseline IAT-II level certification (at proposal submission).
b. Demonstrated experience with system and network security implementation and management.
c. Demonstrated experience with the RMF.

H.1.5 DC3/TSD TECHNICAL TASK LEAD

It is required that the DC3/TSD Technical Task Lead possesses the following qualifications:

a. Demonstrated experience providing technical direction and oversight on multiple ongoing projects.
b. Demonstrated experience in the design, development, and implementation of advanced cyber technologies using high level programming languages.
c. Demonstrated knowledge of Agile and Waterfall development methodologies.
d. Demonstrated experience in testing and evaluation of software, hardware and processes.
e. Knowledge of digital forensics, cyber threat analysis, and open source technology.

It is desired that the DC3/TSD Technical Task Lead possess the following qualifications:

a. Demonstrated knowledge of the DoD and AF policies as it relates to technology development and testing.
b. Demonstrated knowledge of RMF
c. Demonstrated experience in the design, development, and implementation of digital forensics, cyber threat analysis, or cyber intelligence technologies.

H.1.6 DC3-AG TECHNICAL TASK LEAD

It is required that the DC3-AG Technical Lead possesses the following qualifications:

a. Demonstrated experience leading technical efforts or supervising teams supporting intelligence analysis requirements.
b. Demonstrated experience supporting the Intelligence Community or related Government, industrial, and academic communities in the areas of intelligence collection and policy, and intelligence systems and capabilities.
c. Demonstrated experience using principles, concepts, and methodologies of intelligence analysis, including but not limited to the use of HUMINT and SIGINT methods.
d. Demonstrated experience developing requirements and methodologies to collect, analyze, manage and present intelligence in support of cyber investigations.
e. Demonstrated experience in writing various analytical reports (e.g. Intelligence Information Reports (IIRs), cyber threat products).

It is desired that the DC3-AG Technical Lead possess the following qualifications:

a. Demonstrated project management experience (e.g. responsible for handling project scope, cost, resources, risk, and schedule).
b. Demonstrated experience analyzing data to build threat profiles enabling proactive LE/CI cyber operations focused on nation-state threat actors.
c. Demonstrated experience implementing or improving operational processes or procedures in the intelligence analysis lifecycle.

H.1.7 DC3/DCISE TECHNICAL TASK LEAD

It is required that the DC3/DCISE Task Lead possesses the following qualifications:

a. Demonstrated experience leading technical efforts and supervising teams supporting intelligence analysis requirements in the area of all-source cyber analysis and reporting.
b. Demonstrated experience with scanning tools (i.e. VirusTotal) to conduct suspicious file scanning; performing queries, pivoting on indicators, and malware analysis on characteristics (MD5, SHA1, file size, file name, file paths, etc.)
c. Demonstrated experience with intelligence analysis processes, including Open Source Intelligence (OSINT) and closed source intelligence gathering, source verification, data fusion, link analysis, and threat actor knowledge.
d. Demonstrated experience conducting malware and network analysis, identifying protocols, persistence mechanisms, encoding techniques and encryption and how they are used by APT threat actors.

It is desired that the DC3/DCISE Task Lead possess the following qualifications:

a. Demonstrated experience leading and training cyber fusion analysts in malware analysis and generating intelligence reports for review by Government leadership and agency executives.
b. Demonstrated project management experience (e.g. responsible for handling project scope, cost, resources, risk, and schedule).

H.2 NON-KEY PERSONNEL

Directorate	Functional Title	Qualifications	Certifications
ITD	Network personnel (defined in AFMAN 33-285)	Position determined	IAT Level II or higher
DC3-AG	Counter Intelligence Analyst/Linguist	Position determined	ILR 2+/2+ or above for Mandarin, Farsi, Arabic, Russian, and Korean.
DC3/DCISE	Cyber Analyst	(desired) Five years' experience in cyber threat analysis. Experience in verbal presentations and writing reports.	One or more of the following qualifications (desired): GXPN: GIAC Exploit Researcher and Advanced Penetration Tester GREM: GIAC Reverse Engineering Malware GCFA: GIAC Certified Forensic Analyst GWAPT: GIAC Web Application Penetration Tester GPEN: GIAC Certified Penetration Tester GCIA: GIAC Certified Intrusion Analyst GCIH: GIAC Certified Incident Handler

H.3 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the CO. Prior to utilizing other than personnel specified in proposals in response to a TOR, the contractor shall notify the Government CO and the COR of the existing TO. This notification shall be no later than *ten* calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute personnel qualifications shall be equal to, or greater than, those of the personnel being substituted. If the Government CO and the COR determine that a proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6 Termination (Cost Reimbursement).

H.4 GOVERNMENT-FURNISHED PROPERTY (GFP)

The Government will provide on-site office facilities and office equipment for contractor personnel at DC3 locations.

H.5 GOVERNMENT-FURNISHED INFORMATION (GFI)

The Government will provide all necessary information, data, and documents to the contractor for work required under this TO. The contractor shall use Government-furnished information, data, and documents only for performing work under this TO, and shall be responsible for returning all Government-furnished information, data, and documents to the Government at the end of the performance period. The contractor shall not release Government-furnished information, data, and documents to outside parties without the prior and explicit consent of the CO.

H.6 SECURITY CONSIDERATIONS

H.6.1 SECURITY REQUIREMENTS

This is a DoD work effort involving access to and the safeguarding of classified information/material. The security policies, procedures and requirements stipulated in the National Industrial Security Program (NISP); National Industrial Security Program Operating Manual (NISPOM) and any supplements thereto are applicable; to include, applicable FAR and DFARS. The contractor shall also comply with DoD 5200.1-R and AF security regulations and guidance.

The contractor shall meet the Government personnel security, information security and physical security requirements at Government CONUS and OCONUS facilities. Additionally, all contractor personnel working in a SCIF are required to have the following:

a. Have undergone an SSBI or SSBI-PR within the last five years that was favorably adjudicated.
b. Have no break, greater than 24 months, in military service, Federal civilian employment or access to classified information under the Industrial Security Program.
c. Possess a current TS security determination.
d. Possess a SCI determination reflected in JPAS or Scattered Castles.

In order to report to a SCIF for the first day of employment, contractor personnel must possess a current TS clearance with a SCI determination reflected in JPAS or Scattered Castles and be formally nominated by their company's security office to be indoctrinated into SCI programs.

Throughout the period of performance, the contractor will be required to adhere to any changes in the security clearance requirements. The Government will notify the contractor in advance of any changes impacting the contract. If any contracted personnel are required to obtain a TS/SCI for access to a SCIF, the contractor shall seek to obtain this clearance within 180 calendar days of assignment to the SCIF. If the contractor is unable to obtain this clearance, the contractor shall:

a. Notify the Government with a written explanation for the delay.
b. Terminate billing for the employee against the contract if required by the Government.

If any contracted personnel employed by the contractor in support of this contract, fail to *maintain* the required security clearance or access, or are involved in an incident which could jeopardize their access to classified material, the contractor shall:

a. Notify the Government of this discrepancy.
b. Remove the employee from the DC3 site.
c. Terminate billing for the employee against the contract.

H.6.2 SECURITY CLEARANCES

At a minimum, all contractor personnel supporting this TO are required to have an active secret clearance. The Government will accept interim Secret clearances on case by case basis. The remaining personnel are required to have a TS/SCI.

a. Key Personnel: 100% are required to have TS/SCI
b. DC3/CFL D/MM Forensic Examiners: 60% are required to have TS/SCI
c. DC3/CFL D/MM Forensic Technicians: 60% are required to have TS/SCI
d. DC3/CFL Evidence Custodians: 60% are required to have TS/SCI
e. DC3-AG Personnel: 100% are required to have TS/SCI (contractors will be required to obtain a CI Polygraph post-employment)
f. DC3/DCISE Personnel: 75% are required to have TS/SCI
g. ITD Personnel: 50% are required to have TS/SCI
h. DC3/TSD Personnel: 50% are required to have TS/SCI
i. BTO Operational Security: 100% Operational Security staff are required to have TS/SCI
j. BTO: 75% are required to have TS/SCI

The Government will accept TS/SCI-eligible personnel at proposal submission. TS/SCI-eligible personnel must have SCI Determination reflected in JPAS or Scattered Castles.

The Government will specify contractor personnel required to support SAP and SAR programs upon award.

The Government retains the right to request removal of contractor personnel, regardless of prior clearance or adjudication status, whose actions while assigned, to this TO conflict with the interests of the Government. The reason for removal will be fully documented in writing by the FEDSIM COR in coordination with the DC3 TPOC.

As specified by the Government, all contractor personnel requiring specific access to intelligence systems require a Counterintelligence Security Polygraphs (CISP).

A DD254 **(Section J, Attachment C)** will be provided at time of award.

H.6.3 AIR FORCE PRIVACY AND SECURITY REQUIREMENTS

This is a DoD work effort involving access to and/or the safeguarding of classified information/material. The security policies, procedures and requirements stipulated in the National Industrial Security Program (NISP) and National Industrial Security Program Operating Manual (NISPOM) and any supplements thereto are applicable. To include, applicable FAR, DFARS and Air Force Federal Acquisition Regulations (AFFARS) security provisions and/or

clauses. AFFARS Clause 5352-204-9000, Notification of Security Activity and Visitor Group Security Agreement (VGSA) is applicable to this effort whenever TO performance occurs on an AF installation or within an AF controlled facility or activity.

This work effort involves the contractor having access to and/or safeguarding of classified information/material and shall require TS clearances with SCI eligibility and other security accesses (Critical Nuclear Weapons Design Information (CNWDI), Restricted Data, Formerly Restricted Data, NATO, SAP, SAR, COMSEC) identified by the DC3 for TO performance. Other work performed under this TO may require lower clearance levels appropriate for TO performance. Contractors having access to and/or safeguarding classified information/material shall require the appropriate security clearance. The security policies, procedures and requirements stipulated in the NISP; NISPOM and supplements thereto are applicable, to include the following security requirements and/or guidance whenever TO performance will occur on a DoD installation or within a DoD controlled facility or activity:

a. The contractor shall possess or acquire a facility clearance equal to the highest classification stated in the above paragraph in accordance with the NISPOM for TO performance.
b. Disclosure of Information: The contractor shall not release to anyone outside the contractor's organization any classified information, regardless of medium (e.g., film, tape, document, etc.), pertaining to any part of this TO or any program related to this TO, unless: (1) The Contracting Officer has given prior written approval; or (2) The information is otherwise in the public domain before the date of release. Request for approval shall identify the specific information to be released, the medium to be used, and the purpose for the release. The contractor shall submit its request to the Contracting Officer at least 45 days before the proposed date for the release. The contractor agrees to include a similar requirement in each subcontract under this TO. Subcontractors shall submit request for authorization to release through the prime contractor to the Contracting Officer.
c. The contractor's procedures for protecting against unauthorized disclosure of information shall not require Department of Defense employees or members of the Armed Forces to relinquish control of their work product, whether classified or not, to the contractor.
d. Prior to beginning operations involving classified information at the Government facility, the contractor must possess, or acquire prior to award of a contract, a facility clearance equal to the highest classification stated on the Contract Security Classification Specification 9, DD Form 254, attached to this solicitation, the contractor shall enter into a security agreement (or understanding) with the local Government security office. This will ensure contractors follow local security procedures while performing at the Government facility. As a minimum, the agreement shall identify the security actions that will be performed: (a) By the Government facility for the contractor, such as providing storage and classified reproduction facilities, guard services, security forms, security reviews under DoD 5220.22-M, classified mail services, security badges, visitor control, and investigating security incidents; and (b) Jointly by the contractor and the installation, such as packaging and addressing classified transmittals, security checks, internal security controls, and implementing emergency procedures to protect classified information.
e. Pursuant to Section 808 of Pub. L. 102-190 (DFAS 204, Subpart 204.402(2)), DoD

employees or members of the Armed Forces who are assigned to or visiting a contractor facility and are engaged in oversight of an acquisition program will retain control of their work product. Classified work products of DoD employees or members of the Armed Forces shall be handled in accordance with DoD 5220.22-M. Contractor procedures for protecting against unauthorized disclosure of information shall not require DoD employees or members of the Armed Forces to relinquish control of their work products, whether classified or not, to a contractor.

f. If a visit to a contractor facility will require access to classified information, the visitors must give the contractor advance written notice.

g. When TO performance will involve classified information, the contracting officer shall ensure that the DD Form 254, Contract Security Classification Specification, includes the complete mailing address of the Information Security Program Manager (ISPM) and the responsible Major Command (MAJCOM) security forces. Promptly after TO award, the contracting officer shall provide a copy of the DD Form 254 to each addressee on the DD Form 254.

h. Work on this project may require that personnel have access to Privacy and other sensitive information. Personnel shall adhere to the Privacy Act, Title 5 of the United States code, section 552a and applicable Client Agency rules and regulations.

i. Contractor personnel shall not divulge or release privacy data or information developed or obtained in the performance of this TO, until made public or specifically authorized by the Government. The contractor shall not use, disclose, or reproduce third party companies' proprietary data, other that as authorized and required in performance of this TO. Personnel working on this project will be required to sign a non-disclosure agreement immediately upon their start on the project, electronic signatures are also acceptable. The contractor's procedures for protecting against unauthorized disclosure of information shall not require Department of Defense employees or members of Armed Forces to relinquish control of their work product, whether classified or not, to the contractor.

j. All Research, Development, Test and Evaluation Projects accomplished by contractor personnel in support of this TO become the Intellectual Property of DC3 and the US Government.

Where classified information/data is involved, the contractor shall comply with the "National Industrial Security Program Operating Manual (NISPOM)" and the DD Form 254 (Contract Security Classification Specification) that is included per DD254 in **Section J, Attachment C** (Ref FAR 52.204-2).

The contractor will be required to comply with all security requirements in accordance with DoD 5200.2-R, Personal Security Program, contractor personnel shall have as a minimum a favorable National Agency Check (NAC) completed before being permitted access to any Government automated IT system.

H.6.4 FOREIGN CONTRACTORS

In accordance with the DD Form 254, foreign firms or foreign-owned firms will not be permitted to participate as prime contractors, unless they have been approved by Defense Security Service (DSS) under the Foreign Ownership, Control, or Influence (FOCI) process to receive a facility

security clearance. In accordance with the National Industrial Security Program Operating Manual (NISPOM) and FOCI, security measures must be established to mitigate the foreign ownership in order to receive a facility security clearance. A foreign-owned company may also be cleared under a Special Security Agreement (SSA). If an SSA-cleared company requires access to prescribed information (e.g., TS/SCI), a National Interest Determination (NID) will be processed and approved to declare that release of information would not harm the national security interests of the United States.

H.6.5 IA WORKFORCE IMPROVEMENT PROGRAM

The contractor shall ensure that personnel accessing information systems have the proper and current IA certification to perform IA functions in accordance with DoD 8570.01-M, IA Workforce Improvement Program.

The contractor shall meet the applicable IA certification requirements, including:

a. DoD-approved IA workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M.
b. Appropriate operating system certification for IA technical positions as required by DoD 8570.01-M.

Upon request by the Government, the contractor shall provide documentation supporting the IA certification status of personnel performing IA functions.

Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing IA functions.

H.7 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.7.1 ORGANIZATIONAL CONFLICT OF INTEREST

a. If a contractor is currently performing work, or anticipates performing work that creates or represents an actual or potential organizational conflict of interest (OCI), the contractor shall immediately disclose this actual or potential OCI to GSA in accordance with FAR Subpart 9.5. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.
b. The contractor is required to complete and sign an OCI Statement **(Section J, Attachment U)**. The contractor must represent either that (1) It is not aware of any facts which create any actual or potential OCI relating to the award of this contract, or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential OCI and has included a mitigation plan in accordance with paragraph (c) below.
c. If the contractor with an actual or potential OCI believes the conflict can be avoided, neutralized, or mitigated, the contractor shall submit a mitigation plan to the Government for review.
d. In addition to the mitigation plan, the FEDSIM CO may require further information from the contractor. The FEDSIM CO will use all information submitted by the contractor, and any other relevant information known to GSA, to determine whether an award to the

contractor may take place, and whether the mitigation plan adequately avoids, neutralizes, or mitigates the OCI.

e. If any such conflict of interest is found to exist, the FEDSIM CO may determine that the conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government and the contractor may be found ineligible for award. Alternatively, the FEDSIM CO may determine that it is otherwise in the best interest of the United States to contract with the contractor and include the appropriate provisions to avoid neutralize, mitigate, or waive such conflict in the contract awarded.

H.7.2 NON DISCLOSURE REQUIREMENTS

If this TO requires the contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall ensure that all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

a. Execute sign (electronic signatures are also acceptable and submit an Employee/Contractor Non-Disclosure Agreement (NDA) Form **(Section J, Attachment G)** prior to the commencement of any work on the TO, and
b. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information.

All proposed replacement contractor personnel also must submit an NDA and be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained by the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

Additionally, all contractor personnel supporting tasks associated with financial management and plans and programming as outlined in **Section J, Attachment T** are required to submit an NDA prior to the commencement of any work on the TO.

H.8 PURCHASING SYSTEMS

The objective of a contractor purchasing system assessment is to confirm it is a Government-approved purchasing system and evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting.

When reviews are conducted of the purchasing system, the contractor shall provide the results of the review to the FEDSIM CO within ten workdays from the date the results are known to the contractor.

H.9 COST ACCOUNTING SYSTEM

The adequacy of the contractor's accounting system and its associated internal control system, as well as contractor compliance with the Cost Accounting Standards (CAS), affect the quality and validity of the contractor data upon which the Government must rely for its management oversight of the contractor and contract performance. The contractor's cost accounting system shall be adequate during the entire period of performance and shall permit timely development of

all necessary cost data in the form required by the contract.

H.10 TRAVEL

H.10.1 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Federal Travel Regulations (FTR) - prescribed by the GSA, for travel in the contiguous U.S.
b. Joint Travel Regulations (JTR), Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

H.10.2 TRAVEL AUTHORIZATION REQUESTS

Before undertaking travel to any Government site or any other site in performance of this TO, the contractor shall have this travel approved by, and coordinated with, the FEDSIM COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long distance travel, the contractor shall prepare a Travel Authorization Request for Government review and approval. Long distance travel will be reimbursed for cost of travel comparable with the FTR, JTR, and DSSR, as applicable.

Requests for travel approval shall:

a. Be prepared in a legible manner.
b. Include a description of the travel proposed including a statement as to purpose.
c. Be summarized by traveler.
d. Identify the TO number.
e. Identify the CLIN and Interagency Agreement account associated with the travel.
f. Be submitted in advance of the travel with sufficient time to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

H.10 TOOLS

The Government may require the contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under the TO. Such requirements will be identified at the time a TOR is issued or may be identified during the course of a TO by the Government or the contractor. If the contractor initiates a purchase within the scope of this TO and the prime contractor has an approved purchasing system, the contractor shall submit to the FEDSIM COR a Request to Initiate Purchase (RIP). If the prime contractor does not have an approved purchasing system, the contractor shall submit to the FEDSIM CO a Consent to

Purchase (CTP). The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP from the COR or an approved CTP from the CO.

H.11 COMMERCIAL SUPPLIER AGREEMENTS

H.11.1 The Government understands that commercial software tools that may be purchased in furtherance of this TO as described in Section C and as contemplated in the Tools and ODC CLINs in Section B (included with final TOR) may be subject to commercial agreements which may take a variety of forms, including without limitation licensing agreements, terms of service, maintenance agreements, and the like, whether existing in hard copy or in an electronic or online format such as "click wrap" or "browse wrap" (collectively, “Supplier Agreements”). For purposes of this TO, the Supplier Agreements are “collateral agreements” within the meaning of the FAR clause at 52.227-14(c)(2).

H.11.2 The contractor shall ensure that any proposed Supplier Agreements allow the associated software and services to be used as necessary to achieve the objectives of this TO. The contractor shall provide all applicable Supplier Agreements to the FEDSIM CO prior to purchase and shall cooperate with the Government, including negotiations with the licensor as appropriate, to ensure compliance with this Section. Without limiting the generality of the foregoing, a compliant Supplier Agreement shall permit all of the following at no extra charge to the Government: (a) access and use by support contractors, including a successor contractor upon termination or expiration of this TO; (b) access and use by employees of other Federal, state and local law enforcement agencies; (c) transfer to a different data center and/or a successor contractor’s cloud; and (d) the creation of derivative works that shall be subject to at least the same rights as set forth in subparagraphs (a) through (c) above. The above rights constitute “other rights and limitations” as contemplated in subparagraph (d) of the FAR clause at 52.227-14, Rights In Data – General (May 2014), Alternate III (Dec 2007).

H.12 NEWS RELEASE

The offeror shall not make any news release pertaining to this procurement without prior Government approval and only in coordination with the FEDSIM CO.

H.13 CONTRACTOR IDENTIFICATION

As stated in 48 CFR 211.106, Purchase Descriptions for Service Contracts, contractor personnel shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel and by displaying distinguishing badges or other visible identification for meetings with Government personnel. Contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.

H.14 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, "the data rights provisions in DFARS 252.227-7013 apply.

H.15 AWARD FEE

See the Award Fee Determination Plan in **Section J, Attachment I.**

H.16 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 United States Code (U.S.C.) 794d, and the Architectural and Transportation Barriers Compliance Board's EIT Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services provided, identify the technical standards applicable to all products and services provided, and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

H.17 CONTRACTOR USE OF GOVERNMENT VEHICLES

In accordance with 41 CFR 101–38.301–1, Contractors' Use and FAR 52.251-2 Interagency Fleet Management Vehicles and Related Services, the Contracting Officer authorizes the contractor to utilize Government owned/leased motor vehicles used for official purposes solely in the performance of this task order. This authorization applies to the contractor and its subcontractors. This authorization is only applicable as long as 1) it is in accordance with FAR 28.307, Insurance Under Cost Reimbursement Contracts, the contractor has the suitable liability insurances per FAR 28.307-2, and 2) the contractor establishes and enforces suitable penalties for their employees/subcontractor employees that use, or authorize the use of Government motor vehicles for unofficial purposes or for other than in the performance of the task order; and any cost or expenses not related to the performance of the task order will not be reimbursed by the Government. The use of the Government owned/leased motor vehicles shall be in accordance with 41 CFR 101-39 and 41 CFR 101-38.301-1.

Prior to any use of a Government motor vehicle for use in the performance of this task order, the DCITA TPOC and COR must be notified, and the DC3 TPOC must approve the use of the Government motor vehicle. The notification and approval shall be done in writing via email.

I.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request the CO will make their full text available. Also, the full text of a provision may be accessed electronically at the FAR website:

http://www.acquisition.gov/far/

FAR	TITLE	DATE
52.203-13	Contractor Code of Business Ethics and Conduct	(Oct 2015)
52.203-14	Display of Hotline Posters (fill in or provide link to client's posters)	(Dec 2007)
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower	(Apr 2014)
52.204-2	Security Requirements	(Aug 1996)
52.204-7 (Provision)	System for Award Management	(Jul 2013)
52.204-9	Personal Identity Verification of Contractor Personnel	(Jan 2011)
52.204.10	Reporting Executive Compensation and First Tier Subcontract Awards	(Oct 2015)
52.204-13	System for Award Management Maintenance	(Jul 2013)
52.204-14	Service Contract Reporting Requirements	(Jan 2014)
52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment	(Aug 2020)
52.215-12	Subcontractor Certified Cost or Pricing Data (Deviation)	(May 2018)
52.215-13	Subcontractor Certified Cost or Pricing Data-Modification (Deviation)	(May 2018)
52.215-21	Requirements for Cost or Pricing Data or Information Other than Cost or Pricing Data – Modifications	(Oct 2010)
52.215-22	Limitations on Pass-Through Charges- Identification of Subcontractor Effort	(Oct 2009)
52.215-23	Limitations on Pass-Through Charges	(Oct 2009)
52.219-8	Utilization of Small Business Concerns	(Oct 2014)
52.219-9	Small Business Subcontracting Plan	(Oct 2014)
52.223-15	Energy Efficiency in Energy Consuming Products	(Dec 2007)
52.223-16	Acquisition of EPEAT®-Registered Personal Computer Products	(Oct 2015)
52.224-1	Privacy Act Notification	(Apr 1984)
52.224-2	Privacy Act	(Apr 1984)
52.225-13	Restrictions on Certain Foreign Purchases	(Jun 2008)

52.227-14	Rights in Data – General	(Dec 2007)
52.227-14	Rights In Data – General Alternate II or III	(May 2014)
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	(Dec 2007)
52.227-17	Rights In Data Special Works	(Dec 2007)
52.227-21	Technical Data Declaration Revision and Withholding of Payment – Major Systems	(May 2014)
52.232-18	Availability of Funds	(Apr 1984)
52.232-20	Limitation of Cost	(Apr 1984)
52.232-22	Limitation of Funds	(Apr 1984)
52.232-40	Providing Accelerated Payment to Small Business Subcontractors (Deviation)	(Dec 2013)
52.239-1	Privacy or Security Safeguards	(Aug 1996)
52.244-6	Subcontracts for Commercial Items	(Apr 2015)
52.246-5	Inspection of Services—Cost-Reimbursement	(Apr 1984)
52.246-25	Limitation of Liability – Services	(Feb 1997)
52.247-14	Contractor Responsibility for Receipt of Shipment	(Apr 1984)
52.247-67	Submission of Transportation Documents for Audit Fill-in: COR, see Section G	(Feb 2006)
52.249-6	Termination (Cost-Reimbursement)	(May 2004)
52.249-14	Excusable Delays	(Apr 1984)
52.251-1	Government Supply Sources	(Apr 2012)

I.1.1 CLAUSES INCORPORATED BY FULL TEXT

52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six months. The Contracting Officer may exercise the option by written notice to the contractor within 30 days of the end of the period of performance.

(End of clause)

52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

a. The Government may extend the term of this contract by written notice to the contractor within 30 days; provided that the Government gives the contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

b. If the Government exercises this option, the extended contract shall be considered to

include this option clause.

c. The total duration of this contract, including the exercise of any options under this clause, shall not exceed 66 months.

(End of clause)

I.2 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at the GSAM website:

https://www.acquisition.gov/gsam/gsam.html/

GSAM	TITLE	DATE
552.204-9	Personal Identity Verification Requirements	(Oct 2012)
552.232.25	Prompt Payment	(Nov 2009)
552.236-75	Use of Premises	(Apr 1984)
552.239-70	Information Technology Security Plan and Security Authorization	(Jun 2011)
552.239-71	Security Requirements for Unclassified Information Technology Resources	(Jan 2012)

I.3 DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENTS (DFARS) CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at Defense Procurement website:

www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html/

DFARS	TITLE	DATE
252.203-7000	Requirements Relating to Compensation of Former DoD Officials	(Sep 2011)
252.203-7005	Representation Relating to Compensation of Former DoD Officials	(Nov 2011)
252.203-7003	Agency Office of the Inspector General	(Dec 2012)
252.204-7000	Disclosure of Information	(Dec 1991)
252.204-7003	Control of Government Personnel Work Product	(Apr 1992)
252.204-7004	Alternate A, Central Contractor Registration	(Sep 2007)
252.204-7012	Safeguarding of Unclassified Controlled Technical Information	(Oct 2016)
252.205-7000	Provision of Information to Cooperative Agreement Holders	(Dec 1991)
252.206-7000	Domestic Source Restriction	(Dec 1991)
252.209-7001	Disclosure of Ownership of Control by the Government of a Terrorist Country	(Jan 2009)

252.209-7002	Disclosure of Ownership or Control by a Foreign Government	(Jan 2009)
252.211-7003	Item Identification and Valuation	(Jun 2013)
252.211-7007	Reporting Government-Furnished Property	(Aug 2012)
252.216-7005	Award Fee	(Feb 2011)
252.223-7004	Drug-Free Work Force	(Sep 1988)
252.227-7013	Rights in Technical Data - Noncommercial Items	(Feb 2014)
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	(Feb 2014)
252.227-7015	Technical Data-Commercial Items	(Feb 2014)
252.227-7016	Rights in Bid or Proposal Information	(Jan 2011)
252.227-7019	Validation of Asserted Restrictions - Computer Software	(Jan 2011)
252.227-7028	Technical Data or Computer Software Previously Delivered to the Government	(Jun 1995)
252.239-7001	Information Assurance Contractor Training and Certification	(Jan 2008)
252.239-7009	Representation of Use of Cloud Computing	(Sep 2015)
252.239-7010	Cloud Computing Services	(Oct 2016)
252.242-7005	Contractor Business Systems	(Feb 2012)
252.242-7006	Accounting for System Administration	(Feb 2012)
252.244-7001	Contractor Purchasing System Administration	(May 2014)
252.245-7002	Reporting Loss of Government Property	(Apr 2012)
252.245-7003	Contractor Property Management System Administration	(Aug 2011)
252.245-7004	Reporting, Reutilization, and Disposal	(Aug 2011)
252.246-7001	Warranty of Data	(Mar 2014)
252.246-7007	Contractor Counterfeit Electronic Part Detection and Avoidance System	(May 2014)

The following attachments are attached, either in full text or electronically at the end of the TO.

J.1 LIST OF ATTACHMENTS

Attachment	Title
A	COR Appointment Letter
B	Monthly Status Report
C	Department of Defense (DD) 254 (electronically attached .pdf)
D	Travel Authorization Template (electronically attached .xls)
E	Consent to Purchase Template (electronically attached .xls)
F	Request to Initiate Purchase Template (electronically attached .xls)
G	Corporate Non-Disclosure Agreement
H	Incremental Funding Chart
I	Award Fee Determination Plan (Electronically Attached)
J	Appendix A Service Levels (Electronically Attached)
K	Acronym List
L	Excel Workbook (Removed at award)
M	Offeror Q&A Template (Removed at award)
N	Corporate Experience Template (Removed at award)
O	Key Personnel Qualification Matrix (Removed at award)
P	Project Staffing Plan Template (Removed at award)
Q	Problem Notification Report
R	Deliverable Acceptance-Rejection Report
S	OCI Mitigation Plan (Electronically Attached)
T	DC3 Non-Disclosure Agreement (NDA)
U	OCI Statement

ATTACHMENT A

COR APPOINTMENT LETTER ATTACHED FOR:
BONNIE HEIDER

MOD 36 Bonnie Heider COR Letter of Appointment (2).pdf

ATTACHMENT B

Monthly Status Report

Attachment
B_Template Monthly S

Task Order GSQ0017AJ0021
MOD PS36
Contract GS00Q09BGD0011

ATTACHMENT H

Incremental Funding Table

Separately Attached

CLIN	CLIN TYPE	COST OVERRUN CEILING	ESTIMATED COST	ESTIMATED BASE FEE or FIXED FEE	ESTIMATED AWARD FEE	TOTAL ESTIMATED	FUNDED COST	FUNDED BASE FEE or FIXED FEE	FUNDED AWARD FEE	TOTAL FUNDED	ADD/REMOVE INCREMENTAL FUNDING	AMOUNT of LOST AWARD FEE	AMOUNT REMOVED from COST & BASE FEE FUNDING after POP (CPAF only)	ADD COST OVERRUN FUNDING	Base Fee/ Fixed Fee Actual %	Award Fee Actual	Total Fee %
0001	LABOR	(b) (4)													(b) (4)		
0002	LABOR																
0003	TRAVEL																
0004	TOOLS																
0005	ODCs																
0006	CAF																
SUB																	
1001	LABOR																
1002	LABOR																
1003	TRAVEL																
1004	TOOLS																
1005	ODCs																
1006	CAF																
SUB																	
2001	LABOR																
2002	LABOR																
2003	TRAVEL																
2004	TOOLS																
2005	ODCs																
2006	CAF																
SUB																	
3001	LABOR																
3002	LABOR																
3003	TRAVEL																
3004	TOOLS																
3005	ODCs																
3006	CAF																
SUB																	
4001	LABOR																
4002	LABOR																
4003	TRAVEL																
4004	TOOLS																
4005	ODCs																
4006	CAF																
SUB																	
TOTAL		(b) (4)				347,479,403.00				(b) (4)							